

**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 защита выпускной квалификационной работы | 10 семестр - 216 часов |

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-NeviskyAY-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:

РПК-1. Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации.

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.

УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде.

УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах).

УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах.

УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни.

УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.

УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности.

УК-10. Способен формировать нетерпимое отношение к проявлению экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности.

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.

ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности.

ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности.

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности.

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности.

ОПК-8. Способен осуществлять подбор, изучение и общение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.

ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов.

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.

ОПК-4.1. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах.

ОПК-4.2. Способен администрировать операционные системы, системы управления базами данных, вычислительные сети.

ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем.

ОПК-4.4. Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем.

ПК-1. Готов к внедрению систем защиты информации автоматизированных систем.

ПК-2. Способен администрировать средства защиты информации в компьютерных системах и сетях.

ПК-3. Способен проводить контроль защищенности информации.

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 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. ПОДГОТОВКА К СДАЧЕ И СДАЧА ОБЩЕПРОФЕССИОНАЛЬНОГО ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

Общепрофессиональный государственный экзамен учебным планом не предусмотрен.

6. ТРЕБОВАНИЯ К ВЫПУСКНЫМ КВАЛИФИКАЦИОННЫМ РАБОТАМ И ПОРЯДКУ ИХ ВЫПОЛНЕНИЯ

6.1. 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».

Примерная тематика ВКР:

1. Разработка комплекса правил, процедур и практических приемов защиты информации в мобильных устройствах;
2. Проектирование системы охранного видеонаблюдения организации с использованием профессиональных графических инструментов;
3. Защита сетевого хранилища средствами Synology NAS от несанкционированного доступа и нарушения целостности данных;
4. Разработка программы специального обследования по выявлению электронных устройств негласного получения информации в защищаемом помещении предприятия;
5. Методика обоснования структуры службы информационной безопасности, функционального разделения обязанностей персонала и степени их дублирования;
6. Разработка технического задания на систему защиты информации в переговорной комнате (конференц-зале) организации от утечки по (конкретный вид ТКУИ) каналу;
7. Обеспечение безопасности информации на объектах критической информационной инфраструктуры;
8. Разработка проекта технической защиты информации на автоматизированном рабочем месте от ее утечки по (конкретный вид) каналу;
9. Разработка программного обеспечения выделения агрегатов рисков по общим угрозам, уязвимостям и активам;
10. Разработка алгоритма поиска сигналов со сложными структурами в процессе радиомониторинга;
11. Сертификация СМИБ по стандарту ГОСТ Р ИСО/МЭК 27001;
12. Разработка проекта системы защиты конфиденциальной информации в организации;
13. Имитационное моделирование сценариев рисков информационной безопасности;

14. Организация программной защиты сервера с использованием возможностей ОС Microsoft Windows;
15. Разработка проекта технической защиты информации в кабинете руководителя организации от утечки по (конкретный вид) каналу;
16. Организация программной защиты веб-сервера с использованием возможностей операционной системы ALT Linux;
17. Разработка программы специальной проверки технических средств и систем организации, обрабатывающих конфиденциальную информацию;
18. Защита локальной вычислительной сети организации от несанкционированного доступа к её ресурсам с использованием маршрутизаторов уровня локальных сетей;
19. Разработка программы специального исследования защищенности ТСПИ и ВТСС в кабинете руководителя от утечки опасных сигналов ПЭМИН;
20. Разработка программы специального исследования защищенности средств ВТСС в конференц-зале от утечки речевой информации по акустоэлектрическому каналу;
21. Оценка защищенности планшетных компьютеров от утечки конфиденциальной информации по каналу ПЭМИ;
22. Разработка программы проведения аттестационных испытаний по оценке защищенности автоматизированного рабочего места от утечки информации по электромагнитному каналу;
23. Разработка технического проекта создания защищаемого помещения в организации;
24. Разработка технического проекта системы защиты информации организации от утечки по постоянно действующим каналам связи;
25. Внедрение системы предотвращения утечки информации в финансово-кредитном учреждении;
26. Администрирование программно-аппаратного комплекса «Соболь» на рабочих станциях в организации;
27. Разработка технического задания на проведение поисковых работ по обнаружению скрытых неизлучающих устройств утечки информации;
28. Администрирование систем безопасности сетевого взаимодействия на основе технологии VPN;
29. Администрирование локальной вычислительной сети организации при использовании сервисов и ресурсов сети интернет.
30. Защита беспроводных подключений к локальной вычислительной сети при использовании точек доступа общего пользования;
31. Методика инвентаризации, классификации и анализа информационных активов организации;
32. Администрирование программно-аппаратного комплекса «Аккорд» на рабочих станциях организации;
33. Инструментальные проверки персонала организации, использующего в работе конфиденциальную информацию;
34. 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);
35. Мониторинг состояния объекта на основе оценки рисков;
36. Обеспечение безопасного подключения рабочих станций (название организации), обрабатывающих конфиденциальную информацию, к сети Интернет;
37. Внедрение методов и способов организации автоматизированного пропускного режима на предприятии;
38. Автоматизация процесса подготовки отчетных документов по результатам проведения инструментального контроля уровня защищенности автоматизированного рабочего места;

39. Защита файлового архива организации средствами операционной системы;
40. Защита сетевого хранилища средствами QNAP NAS от несанкционированного доступа и нарушения целостности данных; 70..
41. Защита сетевого хранилища организации;
42. Защита локальной вычислительной сети организации с использованием IDS/IPS систем;
43. Аттестация системы информационной безопасности государственной информационной системы;
44. Защита информации в вычислительной сети организации с использованием возможностей провайдеров;
45. Программная защита информационной системы организации на основе возможностей операционной системы;
46. Защита интеллектуальной собственности в организации.
47. Обеспечение безопасности сетевого взаимодействия с использованием технологии OpenVPN;
48. Применение межсетевых экранов экспертного уровня для защиты ресурсов локальной вычислительной сети в организации;
49. Оценка защищенности автоматизированного рабочего места от утечки конфиденциальной информации по каналу ПЭМИ при применении средств активной защиты;
50. Внедрение системы антивирусной защиты в организации;
51. Разработка программы проведения радиомониторинга в защищаемом помещении организации;
52. Разработка программы проведения аттестационных испытаний по оценке защищенности переговорной комнаты (конференц-зала и т.д.) от утечки информации по акустическому (виброакустическому, акустоэлектрическому, электроакустическому) каналу;
53. Защита от несанкционированных проводных подключений к локальной сети (название организации);
54. Оценка защищенности АРМ от утечки конфиденциальной информации по каналу ПЭМИ матрицы монитора;
55. Организация аудита информационной безопасности организации с использованием специального программного обеспечения;
56. Методы и технологии обнаружения скрытых контейнеров в сообщениях методами статистического анализа;
57. Организация программной защиты веб-сервера с использованием возможностей операционной системы AstraLinux.
58. Администрирование системы резервного копирования для защиты информационных активов организации;
59. Моделирование уязвимостей протоколов защиты SSL;
60. Моделирование уязвимостей протоколов защиты информации в сетях Kerberos;
61. Аудит безопасности локальной вычислительной сети организации с использованием сканера безопасности;
62. Автоматизация процессов менеджмента информационной безопасности в организации;
63. Разработка квестов по обучению технологии проникновения в защищенную сеть (этичный хакинг);
64. Анализ технологий разработки смарт-контрактов и выявление их уязвимостей;
65. Технологии реверсинга (обратного программирования) и их применение при исследовании недекларированных функций программного обеспечения;
66. Асимметричные криптосистемы и методы обеспечения конфиденциальности при их использовании;

67. Обеспечение информационной безопасности Интернета вещей в цифровой экономике;
68. Оценка опасности уязвимостей беспроводных информационных технологий на основе Kali Linux;
69. Организация режима защиты конфиденциальной информации на предприятии государственного сектора экономики;
70. Анализ методов обеспечения информационной безопасности в беспроводных сетях передачи информации;
71. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере общественной организации);
72. Организация специальных инструментальных проверок персонала для противодействия инсайдерству в финансовом учреждении (на предприятии энергетики);
73. Инвентаризация и классификация информационных активов организации при оценке рисков;
74. Инвентаризация и классификация информационных активов организации при оценке рисков;
75. Технология защиты авторских прав мультимедийных файлов с использованием цифровых водяных знаков;
76. Методика генерации сценариев целевых атак на информационные системы;
77. Организация программной защиты файлового сервера с использованием возможностей операционной системы AstraLinux;
78. Оценка опасности уязвимостей смарт-контрактов в технологии блокчейн;
79. Автоматизированный выбор мер и средств контроля и управления по заданным рискам с использованием нейронных сетей;
80. Оценка защищенности помещения от утечки речевой информации по линиям охранно-пожарной сигнализации;
81. Внедрение системы сбора и корреляции событий информационной безопасности в финансово-кредитном учреждении;
82. Разработка системы диагностики наличия вредоносного программного обеспечения («в локальной сети организации» или «на сетях IoT-устройств» или «в промышленной сети организации»);
83. Проведение аудита информационной безопасности организации с использованием сканера безопасности;
84. Расследование инцидентов информационной безопасности в организации;
85. Разработка и внедрение электронной подписи в документооборот организации;
86. Разработка средств автоматизации для контроля защищенности автоматизированных систем по требованиям безопасности информации;
87. Разработка программы проведения специального обследования помещения организации по выявлению акустопараметрического канала утечки информации;
88. Организация программной защиты файлового сервера с использованием возможностей операционной системы ALT Linux;
89. Разработка программы специального обследования по выявлению временно отключенных электронных устройств негласного получения информации в защищаемом помещении предприятия;
90. Организация центра управления информационной безопасностью в финансово-кредитном учреждении;
91. Внедрение системы мониторинга информационной безопасности в финансово-кредитном учреждении;
92. Диагностика стеганографических возможностей и противодействие им при реализации информационных процессов в организации;
93. Моделирование угроз персональным данным в организации;

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

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

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

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

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

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

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

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

102. Моделирование уязвимостей протоколов защиты TLS;.

6.2. 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.

6.3. 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 студента 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..

6.4. 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)..

6.5. 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.

6.6. Процедура защиты ВКР

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

6.7. 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 | 30 |
| | | 4 | | |
| | | 3 | | |
| 2 | Доклад и демонстрационный материал | 5 | <ul style="list-style-type: none"> - 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 | <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, допускает ошибки в использовании профессиональной терминологии;</p> | |
| | | 2 | <p>- доклад отличается поверхностной аргументацией основных положений;</p> <p>- логичность и последовательность</p> | |

| | | | | |
|---|------------------------------|---|---|----|
| | | | <p>построения доклада нарушены;</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 и логически непоследовательно, показывает слабые знания предмета выпускной квалификационной работы;</p> | |
| 3 | Отзыв руководителя о работе | 5 | на основе отзыва руководителя по решению ГЭК | 15 |
| 4 | | | | |
| 3 | | | | |
| 4 | Ответы на вопросы членов ГЭК | 5 | обучающийся отвечает на вопросы грамотным языком, ясно, чётко и понятно; вопросы, задаваемые членами ГЭК, не вызывают у обучающегося существенных затруднений; | 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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГИА

При подготовке к ГИА студент может воспользоваться

7.1 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. 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.

4. Бабаш, А. В. Криптографические методы защиты информации. Т.3 : учебно-методическое пособие по специальности 080801 "Прикладная информатика" и другим междисциплинарным специальностям / А. В. Бабаш. – 2-е изд. – М. : РИОР : ИНФРА-М, 2014. – 216 с. – (Высшее образование. Бакалавриат). – ISBN 978-5-369-01304-5.

5. 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.

6. 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.

7. 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.

8. Кибербезопасность цифровой индустрии : теория и практика функциональной устойчивости к кибератакам / Д. П. Зегжда, Е. Б. Александрова, М. О. Калинин, [и др.] ; ред. Д. П. Зегжда. – Москва : Горячая Линия-Телеком, 2020. – 560 с. – Авторы указаны на обороте тит. л. – ISBN 978-5-9912-0827-7.

9. Галатенко, В.А. Стандарты информационной безопасности. Курс лекций : учебное пособие для вузов по специальностям в области информационных технологий / В.А. Галатенко ; Ред. В. Б. Бетелин. – 2-е изд. – М. : Интернет-Ун-т информ. технологий, 2012. – 264 с. – (Основы информационных технологий). – ISBN 978-5-9556-0053-6.

10. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие для среднего профессионального образования по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин. – М. : Форум : ИНФРА-М, 2012. – 416 с. – (Профессиональное образование). – ISBN 978-5-8199-0331-5.

11. Capture the Flag [CTF]. Игровые модели подготовки специалистов в сфере компьютерной безопасности : [учебно-методическое пособие для преподавателей] / А. Ю. Егоров, А. С. Минзов, А. Ю. Невский, О. Р. Баронов, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ). – М. : ВНИИгеосистем, 2018. – 72 с. – ISBN 978-5-8481-0232-1.

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

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

7.2 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

7.3 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>

8. 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, Лекционная аудитория | 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-507, Преподавательская | стол преподавателя, компьютер персональный, 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 |
| Помещения для консультирования | М-511, Учебная аудитория | стол преподавателя, парта, стул, экран, мультимедийный проектор, доска |

| Тип помещения | Номер аудитории, наименование | Оснащение |
|---|---|--|
| | | маркерная, компьютер персональный |
| Помещения для консультирования | М-506, Преподавательская | стол преподавателя, компьютер персональный, 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 |