



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Магнитогорский государственный технический университет им. Г.И. Носова»



**ПРОГРАММА  
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

Направление подготовки (специальность)  
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы  
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном  
исполнении"

Уровень высшего образования - специалитет

Форма обучения  
очная

Институт/ факультет    Институт энергетики и автоматизированных систем  
Кафедра                    Информатики и информационной безопасности

Магнитогорск  
2024 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности  
09.02.2024, протокол № 4

Зав. кафедрой  И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС  
13.02.2024 г. протокол № 4

Председатель  В.Р. Храмшин

Рабочая программа составлена:

зав. кафедрой ИиИБ, д-р техн. наук  И.И. Баранкова

Рецензент:

Начальник отдела информационной безопасности "КУБ" (АО),

 М.М. Блинецов

## 1. Общие положения

Государственная итоговая аттестация проводится государственными экзаменационными комиссиями в целях определения соответствия результатов освоения обучающимися образовательных программ соответствующим требованиям федерального государственного образовательного стандарта.

Специалист по специальности 10.05.03 Информационная безопасность автоматизированных систем в соответствии с специализацией образовательной программы «Разработка автоматизированных систем в защищенном исполнении» должен быть подготовлен к решению задач профессиональной деятельности следующих типов:

- научно-исследовательский;
- проектный;
- контрольно-аналитический;
- организационно-управленческий;
- эксплуатационный.

В соответствии с задачами профессиональной деятельности выпускник на государственной итоговой аттестации должен показать соответствующий уровень освоения следующих компетенций:

Универсальные компетенции

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

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

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

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

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

УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и 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 проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности

Общепрофессиональные компетенции:

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 программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

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

ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные 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;

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах 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 создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

ОПК-8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;

ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем;

ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;

ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;

ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;

ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;

ОПК-16 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-8.1. Способен обосновывать целесообразность создания автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации;

ОПК-8.2. Способен обеспечивать и осуществлять разработку проектных и организационных решений, документирование системы защиты информации автоматизированной системы в защищенном исполнении;

ОПК-8.3. Способен организовывать и обеспечивать информационную безопасность процесса создания автоматизированной системы в защищенном исполнении;

Профессиональные компетенции:

ПК-1 Способен проводить анализ безопасности компьютерных систем

ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей

ПК-3 Способен анализировать причины возникновения компьютерных инцидентов

ПК-3.3 Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов

ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей

ПК-5 Способен проводить аттестацию объектов на соответствие требованиям по защите информации

ПК-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем

ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах

На основании решения Ученого совета университета от 15.02.2023 (протокол № 3) государственные аттестационные испытания по специальности 10.05.03 Информационная безопасность автоматизированных систем проводятся в форме:

– государственного экзамена;

– защиты выпускной квалификационной работы.

К государственной итоговой аттестации допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по данной образовательной программе.

## **2. Программа и порядок проведения государственного экзамена**

Согласно учебному плану подготовка к сдаче и сдача государственного экзамена проводится в период с 17.12.2028 по 30.12.2028. Для проведения государственного экзамена составляется расписание экзамена и предэкзаменационных консультаций (консультирование обучающихся по вопросам, включенным в программу государственного экзамена).

Государственный экзамен проводится на открытых заседаниях государственной экзаменационной комиссии в специально подготовленных аудиториях, выведенных на время экзамена из расписания. Присутствие на государственном экзамене посторонних лиц допускается только с разрешения председателя ГЭК.

Обучающимся и лицам, привлекаемым к государственной итоговой аттестации, во время ее проведения запрещается иметь при себе и использовать средства оперативной и мобильной связи.

Государственный экзамен проводится в два этапа:

- на первом этапе проверяется сформированность общекультурных компетенций;
- на втором этапе проверяется сформированность общепрофессиональных и профессиональных компетенций в соответствии с учебным планом.

#### ***Подготовка к сдаче и сдача первого этапа государственного экзамена***

Первый этап государственного экзамена проводится в форме компьютерного тестирования. Тест содержит вопросы и задания по проверке общекультурных компетенций соответствующего направления подготовки/ специальности. В заданиях используются следующие типы вопросов:

- выбор одного правильного ответа из заданного списка;
- восстановление соответствия.

Для подготовки к экзамену на образовательном портале за три недели до начала испытаний в блоке «Ваши курсы» становится доступным электронный курс «Демо-версия. Государственный экзамен (тестирование)». Доступ к демо-версии осуществляется по логину и паролю, которые используются обучающимися для организации доступа к информационным ресурсам и сервисам университета.

Первый этап государственного экзамена проводится в компьютерном классе в соответствии с утвержденным расписанием государственных аттестационных испытаний.

Блок заданий первого этапа государственного экзамена включает 13 тестовых вопросов. Продолжительность экзамена составляет 30 минут.

Результаты первого этапа государственного экзамена определяются оценками «зачтено» и «не зачтено» и объявляются сразу после приема экзамена.

Критерии оценки первого этапа государственного экзамена:

– на оценку **«зачтено»** – обучающийся должен показать, что обладает системой знаний и владеет определенными умениями, которые заключаются в способности к осуществлению комплексного поиска, анализа и интерпретации информации по определенной теме; установлению связей, интеграции, использованию материала из разных разделов и тем для решения поставленной задачи. Результат не менее 50% баллов за задания свидетельствует о достаточном уровне сформированности компетенций;

– на оценку **«не зачтено»** – обучающийся не обладает необходимой системой знаний и не владеет необходимыми практическими умениями, не способен понимать и интерпретировать освоенную информацию. Результат менее 50% баллов за задания свидетельствует о недостаточном уровне сформированности компетенций.

#### ***Подготовка к сдаче и сдача второго этапа государственного экзамена***

Ко второму этапу государственного экзамена допускается обучающийся, получивший оценку «зачтено» на первом этапе.

Второй этап государственного экзамена проводится в письменной форме.

Второй этап государственного экзамена включает 2 теоретических вопроса и 1 практических задания. Продолжительность экзамена составляет 4 часа

Результаты второго этапа государственного экзамена определяются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в день приема экзамена.

Критерии оценки второго этапа государственного экзамена:

– на оценку **«отлично»** (5 баллов) – обучающийся должен показать высокий уровень сформированности компетенций, т.е. показать способность обобщать и оценивать информацию, полученную на основе исследования нестандартной ситуации; использовать сведения из различных источников; выносить оценки и критические суждения, основанные на прочных знаниях;

– на оценку **«хорошо»** (4 балла) – обучающийся должен показать продвинутый уровень сформированности компетенций, т.е. продемонстрировать глубокие прочные знания и развитые практические умения и навыки, умение сравнивать, оценивать и выбирать методы решения заданий, работать целенаправленно, используя связанные между собой формы представления информации;

– на оценку **«удовлетворительно»** (3 балла) – обучающийся должен показать базовый уровень сформированности компетенций, т.е. показать знания на уровне воспроизведения и объяснения информации, профессиональные, интеллектуальные навыки решения стандартных задач.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся не обладает необходимой системой знаний, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

Результаты второго этапа государственного экзамена объявляются на следующий рабочий день после проведения экзамена.

Обучающийся, успешно сдавший государственный экзамен, допускается к выполнению и защите выпускной квалификационной работе.

## **2.1 Содержание государственного экзамена**

### ***2.1.1 Перечень тем, проверяемых на первом этапе государственного экзамена***

1. Философия, ее место в культуре
2. Исторические типы философии
3. Проблема идеального. Сознание как форма психического отражения
4. Особенности человеческого бытия
5. Общество как развивающаяся система. Культура и цивилизация
6. История в системе гуманитарных наук
7. Цивилизации Древнего мира
8. Эпоха средневековья
9. Новое время XVI-XVIII вв.
10. Модернизация и становление индустриального общества во второй половине XVIII – начале XX вв.
11. Россия и мир в XX – начале XXI в.
12. Новое время и эпоха модернизации
13. Спрос, предложение, рыночное равновесие, эластичность
14. Основы теории производства: издержки производства, выручка, прибыль

15. Основные макроэкономические показатели
16. Макроэкономическая нестабильность: безработица, инфляция
17. Предприятие и фирма. Экономическая природа и целевая функция фирмы
18. Конституционное право
19. Гражданское право
20. Трудовое право
21. Семейное право
22. Уголовное право
23. Я и моё окружение (на иностранном языке)
24. Я и моя учеба (на иностранном языке)
25. Я и мир вокруг меня (на иностранном языке)
26. Я и моя будущая профессия (на иностранном языке)
27. Страна изучаемого языка (на иностранном языке)
28. Формы существования языка
29. Функциональные стили литературного языка
30. Проблема межкультурного взаимодействия
31. Речевое взаимодействие
32. Деловая коммуникация
33. Основные понятия культурологии
34. Христианский тип культуры как взаимодействие конфессий
35. Исламский тип культуры в духовно-историческом контексте взаимодействия
36. Теоретико-методологические основы командообразования и саморазвития
37. Личностные характеристики членов команды
38. Организационно-процессуальные аспекты командной работы
39. Технология создания команды
40. Саморазвитие как условие повышения эффективности личности
41. Диагностика и самодиагностика организма при регулярных занятиях физической культурой и спортом
42. Техническая подготовка и обучение двигательным действиям
43. Методики воспитания физических качеств.
44. Виды спорта
45. Классификация чрезвычайных ситуаций. Система чрезвычайных ситуаций
46. Методы защиты в условиях чрезвычайных ситуаций

***2.1.2 Перечень теоретических вопросов, выносимых на второй этап государственного экзамена***

Теоретические вопросы:

1. Требования по защите информации от НСД для АС.
2. Требования к показателям защищенности СВТ от НСД.
3. Идентификация и аутентификация пользователей. Типовые схемы идентификации и аутентификации пользователя.
4. Аудит событий безопасности.
5. Управление политикой безопасности.
6. Классификация и общая характеристика программно-аппаратных средств защиты информации.
7. Модель защищенной компьютерной системы. Управление доступом к информации в КС.

8. Сравнительный анализ основных механизмов защиты информации в ИС, обеспечения разграничения и контроля доступа пользователей к техническим средствам вычислительной сети на примере АПМДЗ «КРИПТОН-ЗАМОК» и СЗИ «Страж NT».
9. Виды атак на MBR и GPT, их принцип действия и возможная защита от них.
10. Виды атак на уровне СУБД и способы защиты от них.
11. Программные закладки.
12. Виды атак на уровне ОС и способы защиты от них.
13. Виды атак на уровне сетевого ПО и способы защиты от них.
14. Характеристики технических каналов утечки информации. Классификация ТКУИ.
15. Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации.
16. Каналы утечки речевой информации.
17. Каналы утечки информации при ее передаче по каналам связи.
18. Технические каналы утечки видовой информации.
19. Технические каналы утечки информации, возникающей при работе вычислительной техники за счет ПЭМИН.
20. Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений.
21. Закладные устройства, их характеристики и защита от них.
22. Основные средства обнаружения ТКУИ и их характеристики.
23. Методы и средства защиты речевой информации.
24. Пассивные и активные методы защиты информации в акустическом канале.
25. Типы микрофонов и их характеристики. Направленные и лазерные микрофоны принципы их работы.
26. Организационно-методические основы инженерно-технической защиты информации.
27. Физические АЭП - преобразователи – источники опасных сигналов.
28. Способы и средства наблюдения в радиодиапазоне.
29. Задачи, решаемые при перехвате сигналов и структура типового комплекса для перехвата.
30. Организация защиты речевой информации.
31. Пассивные средства защиты ВП.
32. Способы и средства прослушивания, слуховая система человека.
33. Стетоскопы и телефонные закладки.
34. Метод ВЧ-навязывания и его применение для добывания информации.
35. Характеристики закладных устройств, затрудняющие их обнаружение.
36. Средства и методы (не меньше двух) обнаружения закладных устройств.
37. Способы подключения и защита телефонной линии.
38. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него.
39. Защита электросети.
40. Подавление диктофонов.
41. Порядок проведения специальной проверки технических средств.
42. Беззаходовые методы прослушивания помещений по ТЛ.

43. Мобильные системы связи и их использование в информационных атаках.
44. Защита информации от атак с помощью сотовых телефонов и диктофонов.
45. Оптические каналы утечки информации (атака и защита).
46. Радиоэлектронные каналы утечки информации.
47. Пассивные и активные методы защиты информации в радиоэлектронном канале.
48. Способы и принципы инженерно технической защиты информации.
49. Утечка информации по ПЭМИН и применяемые меры защиты.
50. Зоны электромагнитного поля и возможности утечки информации.
51. Контролируемая зона и критерий защищённости СВТ.
52. Понятие системы ЗИ. Дестабилизирующие факторы для СЗИ. Системный подход и его принципы.
53. Рационализация расходов на информацию и ее защиту.
54. Классификация СЗИ.
55. Угрозы безопасности АС. Случайные грозы.
56. Угрозы безопасности АС. Преднамеренные угрозы.
57. Оценка угроз безопасности АС.
58. Методы и модели анализа угроз (Процесс НСД).
59. Эмпирический подход к оценке уязвимости информации. Модель с полным перекрытием.
60. Модель нарушения физической целостности информации.
61. Модель несанкционированного получения информации.
62. Требования к СЗИ.
63. Система общеметодологических принципов ЗИ.
64. Понятие сложной системы и основные признаки.
65. Жизненный цикл АС.
66. Модель нарушителя, классификация уровней.
67. Методика использования метода экспертных оценок.
68. Основные концептуальные требования к задачам защиты.
69. Центральная задача теории защиты информации
70. Множество функций защиты информации.

### ***2.1.3 Перечень практических заданий, выносимых на второй этап государственного экзамена***

1. Графический метод расчета радиуса зоны R2 для СВТ.
2. Для представленной схемы ВП выбрать контрольные точки и разработать схемы измерений по акустическому каналу для этих КТ.
3. Для представленной схемы ВП выбрать контрольные точки и разработать схемы измерений по вибрационному каналу для этих КТ.
4. Инструментально-расчетный метод для оценки разборчивости речи.
5. Математическая модель утечки речевой информации по акустическому каналу.
6. Математическая модель утечки речевой информации по виброакустическому каналу.
7. Математическая модель утечки речевой информации по каналам, использующим перехват электромагнитных и электрических сигналов.

8. Вывести расчетные соотношения для случая амплитудной модуляции при использовании оптимального синхронного детектирования сигналов.
9. Вывести расчетные соотношения для случая амплитудной модуляции при использовании оптимальной фильтрации сигналов.
10. Вывести расчетные соотношения для случая частотной модуляции.
11. Обосновать расчетные соотношения для определения дальности перехвата речевой информации.
12. Рассчитать коэффициент затухания электромагнитного поля.
13. Определить коэффициент затухания электромагнитного поля с учетом влияния экранирующих элементов конструкций здания.
14. Математическая модель утечки речевой информации по лазерному каналу.
15. Математическая модель снижения амплитуды колебаний оконного стекла при использовании вязких пленок.
16. Математическая модель снижения амплитуды колебаний оконного стекла при использовании двухкамерного стеклопакета.
17. Математическая модель снижения амплитуды колебаний оконного стекла при использовании нескольких реализуемых способов.
18. Определить возможность аппаратуры разведки по перехвату цифровой речевой информации расчетным методом.
19. Рассчитать показатель защищенности технических средств обработки и передачи цифровой речи по каналу ПЭМИ.
20. Рассчитать показатель защищенности цифровой речи в радиоканале.
21. Оценить качество шумовых маскирующих помех для защиты речевой информации от утечки по акустическому каналу.
22. Определить огибающий спектр маскирующей помехи для средств активной защиты акустической речевой информации.
23. Оценить качество средств виброакустической защиты расчетным методом.
24. Оценить качество шумовых маскирующих помех для защиты речевой информации от утечки по каналам ПЭМИ и каналам высокочастотного облучения и навязывания расчетным методом.

#### **2.1.4 Перечень рекомендуемой литературы для подготовки к государственному экзамену**

##### **а) Основная литература:**

1. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2024. — 216 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2131865> (дата обращения: 27.04.2024). – Режим доступа: по подписке.
2. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2023. — 602 с. — (Среднее профессиональное образование). — DOI 10.12737/1942679. - ISBN 978-5-16-018253-7. - Текст : электронный. - URL:

- <https://znanium.com/catalog/product/1942679> (дата обращения: 27.04.2024). – Режим доступа: по подписке.
3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544290> (дата обращения: 27.04.2024).
  4. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544029> (дата обращения: 27.04.2024).
  5. Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом : учебное пособие для вузов / Е. А. Войниканис ; под редакцией М. А. Федотова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 57 с. — (Высшее образование). — ISBN 978-5-534-17204-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544885> (дата обращения: 27.04.2024).
  6. Панарина, М. М. Корпоративная безопасность: система управления рисками и комплаенс в компании : учебное пособие для вузов / М. М. Панарина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 155 с. — (Высшее образование). — ISBN 978-5-534-16725-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544645> (дата обращения: 27.04.2024).
  7. Толстобров, А. П. Управление данными : учебное пособие для вузов / А. П. Толстобров. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 272 с. — (Высшее образование). — ISBN 978-5-534-14162-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544036> (дата обращения: 27.04.2024).
  8. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/537248> (дата обращения: 27.04.2024).
  9. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539995> (дата обращения: 27.04.2024).
  10. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 357 с. — (Высшее образование). —

- ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/555950> (дата обращения: 27.04.2024).
11. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/538066> (дата обращения: 27.04.2024).
  12. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536453> (дата обращения: 27.04.2024).
  13. Баранкова, И. И. Разработка БД в MS SQL Server с использованием SSMS : учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2018. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2021> (дата обращения: 27.04.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
  14. Баранкова, И. И. Системы контроля и управления доступом : практикум [для вузов] / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2020. - 1 CD-ROM. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2913> (дата обращения: 27.04.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
  15. Баранкова, И. И. Техническая защита информации. Лабораторный практикум : учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/1747> (дата обращения: 27.04.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
  16. Коновалов, М. В. Методы проектирования защищенных распределительных информационных систем : учебное пособие [для вузов] / М. В. Коновалов ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2021. - 1 CD-ROM. - ISBN 978-5-9967-2275-4. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/3127> (дата обращения: 27.04.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
  17. Мазнин, Д. Н. Администрирование компьютерных сетей : учебное пособие [для вузов] / Д. Н. Мазнин, Ю. А. Мазнина. - Магнитогорск : МГТУ им. Г. И. Носова, 2023. - 1 CD-ROM. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/21027> (дата обращения: 27.04.2024). - ISBN 978-5-9967-2906-7. - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
  18. Михайлова, У. В. Безопасность корпоративной инфраструктуры : практикум [для вузов] / У. В. Михайлова, М. В. Афанасьева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2021. - 1 CD-ROM. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/3254> (дата обращения: 27.04.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
  19. Организация ЭВМ и вычислительных систем : практикум [для вузов] / И. И. Баранкова, У. В. Михайлова, О. В. Пермякова, Г. И. Лукьянов ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2021. - 1 CD-ROM. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/20755> (дата обращения:

- ния: 27.04.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
20. Организация обработки и защиты ПДН в вузе : учебное пособие [для вузов] / Д. Н. Мазнин, И. И. Баранкова, У. В. Михайлова, Д. А. Илларионова ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - ISBN 978-5-9967-1736-1. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2690> (дата обращения: 27.04.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
  21. Развертывание и настройка виртуальных сетей : учебное пособие [для вузов] / [сост.: В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2388> (дата обращения: 27.04.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
  22. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин [и др.] ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2400> (дата обращения: 27.04.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

**с) Программное обеспечение и Интернет-ресурсы:**

1. Банк данных угроз безопасности информации [Электронный ресурс] – Режим доступа: <https://bdu.fstec.ru> .– Загл. с экрана. Яз. рус.
2. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: <https://www.itsec.ru> – Загл. с экрана. Яз. рус.
3. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: <http://www.osp.ru/lan/> Издательство «Открытые системы. СУБД». <http://www.osp.ru/os/>– Загл. с экрана. Яз. рус.

**Профессиональные базы данных и информационные справочные системы**

| Название курса  | Ссылка  |
|---|---|
| Электронная база периодических изданий East View Information Services, ООО  | <a href="https://dlib.eastview.com/">https://dlib.eastview.com/</a>   |
| Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)  | URL:<br><a href="https://elibrary.ru/project_risc.asp">https://elibrary.ru/project_risc.asp</a>   |
| Архив научных журналов «Национальный электронно-информационный конкорциум» (НП НЭИКОН)  | <a href="https://arch.neicon.ru/xmlui/">https://arch.neicon.ru/xmlui/</a>   |
| Российская Государственная библиотека. Каталоги   | <a href="https://www.rsl.ru/ru/4readers/catalogues/">https://www.rsl.ru/ru/4readers/catalogues/</a>   |
| Электронные ресурсы библиотеки МГТУ им. Г.И. Носова   | <a href="https://host.megaprolib.net/MP0109/Web">https://host.megaprolib.net/MP0109/Web</a>   |
| Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите | <a href="https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053">https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053</a> |

|   |   |
|---|---|
| Банк данных угроз безопасности информации [Электронный ресурс] – Режим доступа: | <a href="https://bdu.fstec.ru">https://bdu.fstec.ru</a> |
|---|---|

## ***2.1.5 Рекомендации обучающимся по подготовке к государственному экзамену***

### *Подготовка к тестированию*

При подготовке к тестированию обучающемуся рекомендуется внимательно изучить структуру теста, оценить объем времени, выделяемого на данный тест, увидеть, ка-кого типа задания в нем содержатся. Следует начинать отвечать на те вопросы, в правильности решения которых нет сомнений, пока не останавливаясь на тех, которые могут вызвать долгие раздумья. Необходимо внимательно читать задания до конца, не пытаясь понять условия «по первым словам» или выполнив подобные задания в предыдущих тестированиях - это приводит к ошибкам в самых легких вопросах. Рекомендуется пропустить вопрос, если обучающийся не знает ответа или не уверен в его правильности, чтобы потом к нему вернуться. Нужно думать только о текущем задании. Как правило, задания в тестах не связаны друг с другом непосредственно, поэтому необходимо концентрироваться на данном вопросе и находить решения, подходящие именно к нему. Обучающийся может не искать сразу правильный вариант ответа, а последовательно исключать те, которые явно не подходят. Метод исключения позволяет в итоге сконцентрировать внимание на одном-двух вероятных вариантах. Следует рассчитывать выполнение заданий так, чтобы осталось время на проверку и доработку. Необходимо свести к минимуму процесс угадывания правильных ответов.

При подготовке к тестированию обучающемуся следует не просто заучивать, необходимо понять логику изложенного материала. Этому способствует составление развернутого плана, таблиц, схем. Большую помощь оказывают опубликованные сборники тестов, Интернет-тренажеры, позволяющие закрепить знания и приобрести соответствующие психологические навыки саморегуляции и самоконтроля.

### *Подготовка к письменному ответу*

Во время подготовки обучающемуся следует правильно составить письменный ответ. Хорошо структурированный ответ должен содержать в себе следующие пункты: определение главных теоретических положений и терминов; примеры по теме вопроса; разные взгляды ученых на заданный вопрос. Обучающемуся рекомендуется подкреплять ответ ссылками на учебные пособия и цитатами ученых, изучающих тему вопроса. Рекомендуется оценить ответ с разных сторон. Если в ответе обучающийся использует сокращения, нужно пояснить, как они расшифровываются. Следует строго отвечать на поставленный вопрос и не пытаться написать лишнюю информацию, при этом ответ на вопрос должен быть максимально полным. Перед написанием ответа на бумаге необходимо составить примерный план ответа на экзаменационный вопрос, чтобы внести в билет всю нужную информацию. Каждый ответ должен иметь логическое завершение и содержать выводы.

### Работа с учебной литературой (конспектом)

При работе с литературой (конспектом) при подготовке к экзамену обещающемуся рекомендуется:

1. Подготовить необходимую информационно-справочную (словари, справочники) и рекомендованную научно-методическую литературу (учебники, учебные пособия) для получения исчерпывающих сведений по каждому экзаменационному вопросу.

2. Уточнить наличие содержания и объем материала в лекциях и учебной литературе для раскрытия вопроса.

3. Дополнить конспекты недостающей информацией по отдельным аспектам, без которых невозможен полный ответ.

Основные виды систематизированной записи прочитанного:

– аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

– планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

– тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

– цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

– конспектирование – краткое и последовательное изложение содержания прочитанного.

4. Распределить весь материал на части с учетом их сложности, составить график подготовки к экзамену.

5. Внимательно прочитать материал конспекта, учебника или другого источника информации, с целью уточнений отдельных положений, структурирования информации, дополнения рабочих записей.

8. Повторно прочитать содержание вопроса, пропуская или бегло просматривая те части материала, которые были усвоены на предыдущем этапе.

9. Прочитать еще раз материал с установкой на запоминание. Запоминать следует не текст, а его смысл и его логику. В первую очередь необходимо запомнить термины, основные определения, понятия, законы, принципы, аксиомы, свойства изучаемых процессов и явлений, основные влияющие факторы, их взаимосвязи. Полезно составлять опорные конспекты.

10. Многократное повторение материала с постепенным «сжиманием» его в объеме способствует хорошему усвоению и запоминанию.

11. В последний день подготовки к экзамену следует проговорить краткие ответы на все вопросы, а на тех, которые вызывают сомнения, остановиться более подробно.

### 3. Порядок подготовки и защиты выпускной квалификационной работы

Выполнение и защита выпускной квалификационной работы является одной из форм государственной итоговой аттестации.

При выполнении выпускной квалификационной работы, обучающиеся должны показать свои знания, умения и навыки самостоятельно решать на современном уровне задачи

своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.

Обучающий, выполняющий выпускную квалификационную работу должен показать свою способность и умение:

- определять и формулировать проблему исследования с учетом ее актуальности;
- ставить цели исследования и определять задачи, необходимые для их достижения;
- анализировать и обобщать теоретический и эмпирический материал по теме исследования, выявлять противоречия, делать выводы;
- применять теоретические знания при решении практических задач;
- делать заключение по теме исследования, обозначать перспективы дальнейшего изучения исследуемого вопроса;
- оформлять работу в соответствии с установленными требованиями.

### **3.1 Подготовительный этап выполнения выпускной квалификационной работы**

#### ***3.1.1 Выбор темы выпускной квалификационной работы***

Обучающийся самостоятельно выбирает тему из рекомендуемого перечня тем ВКР, представленного в приложении 1. Обучающийся (несколько обучающихся, выполняющих ВКР совместно), по письменному заявлению, имеет право предложить свою тему для выпускной квалификационной работы, в случае ее обоснованности и целесообразности ее разработки для практического применения в соответствующей области профессиональной деятельности или на конкретном объекте профессиональной деятельности. Утверждение тем ВКР и назначение руководителя утверждается приказом по университету.

#### ***3.1.2 Функции руководителя выпускной квалификационной работы***

Для подготовки выпускной квалификационной работы обучающемуся назначается руководитель и, при необходимости, консультанты.

Руководитель ВКР помогает обучающемуся сформулировать объект, предмет исследования, выявить его актуальность, научную новизну, разработать план исследования; в процессе работы проводит систематические консультации.

Подготовка ВКР обучающимся и отчет перед руководителем реализуется согласно календарному графику работы. Календарный график работы обучающегося составляется на весь период выполнения ВКР с указанием очередности выполнения отдельных этапов и сроков отчетности по выполнению работы перед руководителем.

### **3.2 Требования к выпускной квалификационной работе**

При подготовке выпускной квалификационной работы обучающийся руководствуется методическими рекомендациями и локальным нормативным актом университета СМК-О-СМГТУ-36-20 Выпускная квалификационная работа: структура, содержание, общие правила выполнения и оформления.

### **3.3 Порядок защиты выпускной квалификационной работы**

Законченная выпускная квалификационная работа должна пройти процедуру нормоконтроля, включая проверку на объем заимствований, а затем представлена руководителю для оформления письменного отзыва. После оформления отзыва руководителя ВКР направляется на рецензию. Рецензент оценивает значимость полученных результатов,

анализирует имеющиеся в работе недостатки, характеризует качество ее оформления и изложения, дает заключение (рецензию) о соответствии работы предъявляемым требованиям в письменном виде.

Выпускная квалификационная работа, подписанная заведующим кафедрой, имеющая рецензию и отзыв руководителя работы, допускается к защите и передается в государственную экзаменационную комиссию не позднее, чем за 2 календарных дня до даты защиты, также работа размещается в электронно-библиотечной системе университета.

Объявление о защите выпускных работ вывешивается на кафедре за несколько дней до защиты.

Защита выпускной квалификационной работы проводится на заседании государственной экзаменационной комиссии и является публичной. Защита одной выпускной работы **не должна превышать 30 минут**.

Для сообщения обучающемуся предоставляется **не более 10 минут**. Сообщение по содержанию ВКР сопровождается необходимыми графическими материалами и/или презентацией с раздаточным материалом для членов ГЭК. В ГЭК могут быть представлены также другие материалы, характеризующие научную и практическую ценность выполненной ВКР – печатные статьи с участием выпускника по теме ВКР, документы, указывающие на практическое применение ВКР, макеты, образцы материалов, изделий и т.п.

В своем выступлении обучающийся должен отразить:

- содержание проблемы и актуальность исследования;
- цель и задачи исследования;
- объект и предмет исследования;
- методику своего исследования;
- полученные теоретические и практические результаты исследования;
- выводы и заключение.

В выступлении должны быть четко обозначены результаты, полученные в ходе исследования, отмечена теоретическая и практическая ценность полученных результатов.

По окончании выступления выпускнику задаются вопросы по теме его работы. Вопросы могут задавать все присутствующие. Все вопросы протоколируются.

Затем слово предоставляется научному руководителю, который дает характеристику работы. При отсутствии руководителя отзыв зачитывается одним из членов ГЭК.

После этого выступает рецензент или рецензия зачитывается одним из членов ГЭК.

Заслушав официальную рецензию своей работы, студент должен ответить на вопросы и замечания рецензента.

Затем председатель ГЭК просит присутствующих выступить по существу выпускной квалификационной работы. Выступления членов комиссии и присутствующих на защите (до 2-3 мин. на одного выступающего) в порядке свободной дискуссии и обмена мнениями не являются обязательным элементом процедуры, поэтому, в случае отсутствия желающих выступить, он может быть опущен.

После дискуссии по теме работы студент выступает с заключительным словом. Этика защиты предписывает при этом выразить благодарность руководителю и рецензенту за проделанную работу, а также членам ГЭК и всем присутствующим за внимание.

### 3.4 Критерии оценки выпускной квалификационной работы

Результаты защиты ВКР определяются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются *в день защиты*.

Решение об оценке принимается на закрытом заседании ГЭК по окончании процедуры защиты всех работ, намеченных на данное заседание. Для оценки ВКР государственная экзаменационная комиссия руководствуется следующими критериями:

- актуальность темы;
- научно-практическое значение темы;
- качество выполнения работы, включая демонстрационные и презентационные материалы;
- содержательность доклада и ответов на вопросы;
- умение представлять работу на защите, уровень речевой культуры.

Оценка **«отлично»** (5 баллов) выставляется за глубокое раскрытие темы, полное выполнение поставленных задач, логично изложенное содержание, качественное оформление работы, соответствующее требованиям локальных актов, высокую содержательность доклада и демонстрационного материала, за развернутые и полные ответы на вопросы членов ГЭК;

Оценка **«хорошо»** (4 балла) выставляется за полное раскрытие темы, хорошо проработанное содержание без значительных противоречий, в оформлении работы имеются незначительные отклонения от требований, высокую содержательность доклада и демонстрационного материала, за небольшие неточности при ответах на вопросы членов ГЭК.

Оценка **«удовлетворительно»** (3 балла) выставляется за неполное раскрытие темы, выводов и предложений, носящих общий характер, в оформлении работы имеются незначительные отклонения от требования, отсутствие наглядного представления работы и затруднения при ответах на вопросы членов ГЭК.

Оценка **«неудовлетворительно»** (2 балла) выставляется за частичное раскрытие темы, необоснованные выводы, за значительные отклонения от требований в оформлении и представлении работы, когда обучающийся допускает существенные ошибки при ответе на вопросы членов ГЭК.

Оценка **«неудовлетворительно»** (1 балл) выставляется за необоснованные выводы, за значительные отклонения от требований в оформлении и представлении работы, отсутствие наглядного представления работы, когда обучающийся не может ответить на вопросы членов ГЭК.

Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение государственного аттестационного испытания, что является основанием для выдачи обучающемуся документа о высшем образовании и о квалификации образца, установленного Министерством образования и науки Российской Федерации.

**Примерный перечень тем выпускных квалификационных работ**

1. Аудит защищенности информационных ресурсов предприятия.
2. Разработка системы защиты корпоративной организации.
3. Разработка системы криптографической защиты данных
4. Разработка средства моделирования угроз безопасности информационной системы.
5. Разработка автоматизированного комплекса для оценки защищенности.
6. Разработка защищенной информационной системы персональных данных.
7. Разработка автоматизированной системы контроля управления доступом.
8. Разработка системы защиты для ИСПДн, подключенной к ГИС.