МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
Директор ИЭиАС
_____ С.И. Лукьянов

26.02.2020 г.

# ПРОГРАММА
# ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

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

Магнитогорск
2019 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
Начальник отдела информационной безопасности «КУБ» (АО)

_____ М.М. Близнецов

**Лист актуализации рабочей программы**

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 1 сентября 2020 г. № 1
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

**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 должен быть подготовлен к решению профессиональных задач в соответствии со специализацией "Обеспечение информационной безопасности распределенных информационных систем" и видам профессиональной деятельности:

- научно-исследовательская;
- проектно-конструкторская;
- контрольно-аналитическая;
- организационно-управленческая;
- эксплуатационная.

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

- способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);
- способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);
- способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);
- способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- 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-5);
- способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);
- 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-7);
- способностью к самоорганизации и самообразованию (ОК-8);
- способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

- способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);
- способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической

статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);
- способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);
- способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);
- способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);
- способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);
- способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).

- способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);
- способностью создавать и исследовать модели автоматизированных систем (ПК-2);
- способностью проводить анализ защищенности автоматизированных систем (ПК-3);
- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);
- способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);
- способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);
- способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);
- способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);
- способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);
- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
- способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);
- способностью участвовать в проектировании средств защиты информации автоматизированной Системы (ПК-13);

- способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);
- способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);
- способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);
- способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);
- способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);
- способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
- способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);
- способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);
- способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);
- способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
- способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);
- способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);
- способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);
- способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

- способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя

информационной безопасности в распределенных информационных системах (ПСК-7.1);
- способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);
- способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);
- способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);
- способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5);
-

На основании решения Ученого совета университета от 29.03.2017 (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 01.06.2019 по 13.06.2019. 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 3 теоретических вопроса и 1 практическое задание. 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.

Результаты второго этапа государственного экзамена объявляются на следующий рабочий день после проведения экзамена (если экзамен проводится в письменной форме).

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 Учебно-методическое обеспечение***

***а) Основная литература:***

1. Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с. http://znanium.com/bookread2.php?book=957144

***б) Дополнительная литература:***

1. Малюк А. А., Горбатов В. С., Королев В. И. и др. Введение в информационную безопасность [Текст]: Учебное пособие для вузов. М. : Горячая линия–Телеком, 2011.
2. Малюк, А. А. Теория защиты информации [Текст]. М.: Горячая линия–Телеком, 2012.
3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2
4. УнижаевН.В.Информационно-аналитическоеобеспечениебезопасностиорга-низации:учебноепособие/УнижаевН.В.–СПб.: Издательскийцентр«Интермедия», 2018.–408с. https://ibooks.ru/reading.php?productid=356934
5. Управление информационными рисками. Экономически оправданная безопасность: Пособие / Петренко С.А., Симонов С.В., - 2-е изд., (эл.) - М.:ДМК Пресс, 2018. - 396 с.http://znanium.com/bookread2.php?book=983162
6. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учеб. пособие для вузов / П.Н. Девянин .— 2-е изд., испр. и доп. — М. : Горячая линия – Телеком, 2013 .— 339 с. — ISBN 978-5-9912-0328-9 . — Режим доступа: http://ibooks.ru/reading.php?productid=344413
7. УнижаевН.В. Информационно-аналитическое обеспечение безопасности орга-низации: учебное пособие/Унижаев Н.В.–СПб.: Издательскийцентр «Интермедия», 2018.–408с. https://ibooks.ru/reading.php?productid=356934
8. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true . - Макрообъект. - ISBN 978-5-9967-1031-7.
9. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных: Учебное пособие / Е.Г. Воробьев – СПб.: Издательский центр «Интермедия», 2016. –432 с. https://ibooks.ru/reading.php?productid=351534
10. Царегородцев А. В., Тараскин М. М. Методы и средства защиты информации в государственном управлении : учебное пособие. — Москва : Проспект, 2017. — 208 с. https://ibooks.ru/reading.php?productid=356008
11. Информационная безопасность при управлении техническими системами: учебное пособие / С.А. Баркалов, О.М. Барсуков, В.Е. Белоусов, К.В. Славнов.—СПб : ИЦ «Интермедия», 2016. —528с.: илл. https://ibooks.ru/reading.php?productid=356935
12. Грибанова-Подкина М.Ю. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования // Вопросы безопасности. — 2017. - № 2. - С.25-34. DOI: 10.7256/2409-7543.2017.2.22065. URL: http://e-notabene.ru/nb/article_22065.html
13. Коваленко, В. В. Проектирование информационных систем [Электронный ресурс]: Учебное пособие / В.В. Коваленко. - М.: Форум: НИЦ ИНФРА-М, 2014. - 320 с. - (Высшее образование). –Режим доступа: http://znanium.com/bookread.php?book=473097 .–Заглавие с экрана. –ISBN 978-5-91134-549-5.
14. Шаньгин, В.Ф Комплексная защита информации в корпоративных системах [Электронный ресурс]: Учебное пособие - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.- (Высшее образование).–Режим доступа: http://znanium.com/bookread.php?book=402686 .–Заглавие с экрана. –ISBN 978-5-8199-0411-4.

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

1. http://www.studentlibrary.ru/catalogue/switch_kit/x2016-034.html
2. Банк данных угроз безопасности информации [Электронный ресурс] – Режим

доступа: https://bdu.fstec.ru .– Загл. с экрана. Яз. рус.

3. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
4. Журнал «Безопасность информационных технологий» : периодич. интернет-изд. URL: http://www.pvti.ru/articles_18.htm – Загл. с экрана. Яз. рус.
5. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
6. «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.
7. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.
8. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru . Яз. рус.
9. Безопасник [Электронный ресурс] – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.
10. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.
11. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/ .– Загл. с экрана. Яз. рус.

**Профессиональные базы данных и информационные справочные системы**

| Название курса | Ссылка |
|---|---|
| Электронная база периодических изданий East View Information Services, ООО «ИВИС» | https://dlib.eastview.com/ |
| Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ) | URL: https://elibrary.ru/project_risc.asp |
| Поисковая система Академия Google (Google Scholar) | URL: https://scholar.google.ru/ |
| Информационная система - Единое окно доступа к информационным ресурсам | URL: http://window.edu.ru/ |
| Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности» | URL: http://www1.fips.ru/ |
| Российская Государственная библиотека. Каталоги | https://www.rsl.ru/ru/4readers/catalogues/ |
| Электронные ресурсы библиотеки МГТУ им. Г.И. Носова | http://magtu.ru:8085/marcweb2/Default.asp |
| Федеральный образовательный портал – Экономика. Социология. Менеджмент | http://ecsocman.hse.ru/ |
| Университетская информационная система РОССИЯ | https://uisrussia.msu.ru |
| Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science» | http://webofscience.com |
| Международная реферативная и полнотекстовая справочная база данных научных изданий «Scopus» | http://scopus.com |

| | |
|---|---|
| Международная база полнотекстовых журналов Springer Journals | http://link.springer.com/ |
| Международная коллекция научных протоколов по различным отраслям знаний Springer Protocols | http://www.springerprotocols.com/ |
| Международная база научных материалов в области физических наук и инжиниринга SpringerMaterials | http://materials.springer.com/ |
| Международная база справочных изданий по всем отраслям знаний SpringerReference | http://www.springer.com/references |
| Международная реферативная база данных по чистой и прикладной математике zbMATH | http://zbmath.org/ |
| Международная реферативная и полнотекстовая справочная база данных научных изданий «Springer Nature» | https://www.nature.com/siteindex |
| Архив научных журналов «Национальный электронно-информационный концорциум» (НП НЭИКОН) | https://archive.neicon.ru/xmlui/ |
| Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России | https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii |
| Информационная система - Банк данных угроз безопасности информации ФСТЭК России | https://bdu.fstec.ru/ |

### 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 указаниями и локальным нормативным актом университета  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.

### 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 значением 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 требовании, 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.

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.

Приложение 1

**Примерный перечень тем выпускных квалификационных работ**

1. Аудит защищенности информационных ресурсов предприятия.
2. Разработка системы защиты корпоративной сети учебного заведения на основе технологии VipNet.
3. Разработка системы криптографической защиты облачного хранилища данных
4. Разработка средства моделирования угроз безопасности информационной системы на основе теории графов.
5. Разработка автоматизированного комплекса для оценки защищенности от утечки по акустическим каналам.
6. Разработка защищенной информационной системы персональных данных.
7. Разработка автоматизированной системы контроля управления доступом.
8. Разработка защищенной корпоративной сети для топливной компании с применением технологии VPN.
9. Разработка системы защиты для ИСПДн, подключенной к ГИС.