10.05.03.07.Б1-2018-ФОС

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»
Институт информационных технологий, машиностроения и автотранспорта

УТВЕРЖДАЮ
Директор ИИТМА
_____ Д.В. Стенин
«22» 04. 2021 20__ г.

Программа итоговой (государственной итоговой) аттестации

Специальность 10.05.03 Информационная безопасность автоматизированных систем
Специализация «Анализ безопасности информационных систем»

Присваиваемая квалификация
"Специалист по защите информации"

Блок 3 «Государственная итоговая аттестация»
«Подготовка к процедуре защиты и защита выпускной квалификационной работы»

Формы обучения
Очная

Кемерово 2021

Программу итоговой (государственной итоговой) аттестации составили

Заведующий кафедрой	Информацинная безопасность		Е.В. Прокопенко

Фонд оценочных средств обсужден на заседании кафедры Информацинная безопасность

Протокол № 6 от 01.03.2021

Зав. кафедрой Информацинная безопасность  Е.В. Прокопенко

Согласовано учебно-методической комиссией по специальности 10.05.03 Информационная безопасность автоматизированных систем

Протокол № 6 от 01.03.2021

Председатель учебно-методической комиссии специальности 10.05.03 Информационная безопасность автоматизированных систем  Е.В. Прокопенко

подпись

Оглавление

1 Общие положения

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

Лицам, успешно прошедшим итоговую (государственную итоговую) аттестацию, выдаются в установленном порядке документы об образовании и о квалификации.

Лицам, не прошедшим итоговую (государственную итоговую) аттестацию или получившим на итоговой (государственной итоговой) аттестации неудовлетворительные результаты, а также лицам, освоившим часть образовательной программы и (или) отчисленным из организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому организацией.

Обучающимся по образовательным программам после прохождения итоговой (государственной итоговой) аттестации предоставляются по их заявлению каникулы в пределах срока освоения соответствующей образовательной программы, по окончании которых производится отчисление обучающихся в связи с получением образования.

Итоговая (государственная итоговая) аттестация направлена на установление соответствия уровня результатов освоения обучающимися основных образовательных программ соответствующим требованиям федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Организации используют необходимые для организации образовательной деятельности средства при проведении государственной итоговой аттестации обучающихся.

Организации вправе применять электронное обучение, дистанционные образовательные технологии при проведении государственных аттестационных испытаний. Особенности проведения государственных аттестационных испытаний с применением электронного обучения, дистанционных образовательных технологий определяются локальными нормативными актами организации. При проведении государственных аттестационных испытаний с применением электронного обучения, дистанционных образовательных технологий организация обеспечивает идентификацию личности обучающихся и контроль соблюдения требований, установленных указанными локальными нормативными актами.

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

Выпускные квалификационные работы по программам специалитета подлежат рецензированию.

Для проведения рецензирования выпускной квалификационной работы указанная работа направляется организацией одному или нескольким рецензентам из числа лиц, не являющихся работниками кафедры, либо факультета (института), либо организации, в которой выполнена выпускная квалификационная работа. Рецензент проводит анализ выпускной квалификационной работы и представляет в организацию письменную рецензию на указанную работу (далее - рецензия).

Если выпускная квалификационная работа имеет междисциплинарный характер, она направляется организацией нескольким рецензентам. В ином случае число рецензентов устанавливается организацией.

Лицо, не прошедшее государственную итоговую аттестацию, может повторно пройти государственную итоговую аттестацию не ранее чем через 10 месяцев и не позднее чем через пять лет после срока проведения государственной итоговой аттестации, которая не пройдена обучающимся. Указанное лицо может повторно пройти государственную итоговую аттестацию не более двух раз.

Для повторного прохождения государственной итоговой аттестации указанное лицо по его заявлению восстанавливается в организации на период времени,

установленный организацией, но не менее периода времени, предусмотренного календарным учебным графиком для государственной итоговой аттестации по соответствующей образовательной программе.

При повторном прохождении государственной итоговой аттестации по желанию обучающегося решением организации ему может быть установлена иная тема выпускной квалификационной работы.

Для обучающихся из числа инвалидов государственная итоговая аттестация проводится организацией с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья.

Обучающийся имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, установленной процедуры проведения государственного аттестационного испытания и (или) несогласии с результатами государственного экзамена.

Апелляция подается лично обучающимся в апелляционную комиссию не позднее следующего рабочего дня после объявления результатов государственного аттестационного испытания. Порядок подачи и рассмотрения апелляций прописан в п. 10 «Положения о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в КузГТУ».

Итоговая (государственная итоговая) аттестация включает:

- Подготовка к процедуре защиты и защита выпускной квалификационной работы

2 Требования к выпускной квалификационной работе, порядку ее выполнения и порядку защиты

Выпускная квалификационная работа (ВКР) выполняется обучающимися самостоятельно в печатном виде и включает при необходимости комплект чертежей формата А1 (допускается для отдельных листов использования нестандартных форматов) и пояснительную записку на листах формата А4 (для отдельных листов допускается использование других форматов) объемом не менее 50 страниц.

На каждом листе графической части в правом нижнем углу должен быть установленной формы штамп (приложение А). По ходу работы соответствующие места в угловом штампе заполняются подписями обучающегося и руководителя.

Все чертежи должны иметь название, при этом размер букв по высоте не должен быть меньше 15 мм. Чертеж должен быть ясным, четким и равномерно заполненным. На каждом листе графической части общая незаполненная площадь должна составлять не более 15 % от общей площади листа. Каждый лист графической части должен иметь единый стиль оформления, а также порядковый номер в правом верхнем углу высотой шрифта не менее 20 мм.

Пояснительная записка – документ, содержащий систематизированные данные, обосновывающие, поясняющие и дополняющие все принятые решения в рамках ВКР, который, помимо текстовой части, должен сопровождаться иллюстрациями, диаграммами, схемами и т.д.

Пояснительная записка должна иметь следующую структуру:

- титульный лист;
- задание на выполнение ВКР;
- календарный план;
- аннотация;
- содержание;
- введение;
- основная часть (по теме ВКР);
- спецчасть (при необходимости);
- список литературы;

- приложения (при необходимости).

На титульном листе пояснительной записки должны быть подписи:

- заведующего кафедрой;
- руководителя ВКР;
- консультанта по нормоконтролю.

Объем и содержание ВКР должно соответствовать индивидуальному заданию, выданным руководителем ВКР после согласования его с заведующим кафедрой. Отклонения от задания возможны при их согласовании с руководителем ВКР.

Работа над ВКР ведется систематически с периодическим представлением результатов руководителю ВКР, а также консультантам для проверки. В ходе выполнения ВКР обучающийся консультируется с руководителем ВКР и консультантами, как при непосредственном взаимодействии, так и с использованием ресурсов ЭИОС КузГТУ, в том числе синхронного и (или) асинхронного взаимодействия посредством сети «Интернет». ВКР считается выполненной в полном объеме, если объем и содержание ВКР соответствует заданию (с учетом внесенных изменений и дополнений), на титульном листе пояснительной записки имеются подписи руководителя ВКР, а также консультантов по соответствующим разделам, листы графической части подписаны руководителем.

При защите ВКР обучающийся развешивает на специально подготовленных стендах листы графической части и выступает с докладом в течение 5-7 минут. В ходе доклада обучающийся располагается непосредственно у листов графической части и указкой показывает на те элементы, о которых он рассказывает. Зачитывать текст доклада не допускается. По окончании доклада обучающийся благодарит членов государственной экзаменационной комиссии за уделенное внимание и предлагает задать вопросы. Каждый член государственной экзаменационной комиссии задает до двух письменных и до двух устных вопросов, на которые обучающийся должен дать ответы. После дачи ответов на заданные вопросы процедура защиты ВКР для обучающегося считается законченной.

3 Критерии и шкала оценки результатов подготовки и защиты выпускной квалификационной работы

Во время защиты обучающемуся задаются вопросы, касающиеся темы ВКР, а также другие вопросы, позволяющие оценить сформированность заявленных компетенций.

Критерии оценивания результатов подготовки и защиты выпускной квалификационной работы (ВКР):

- обучающийся сделал уверенный доклад по ВКР, дал правильные и полные ответы более чем на 85 % заданных вопросов – 85…100 баллов;
- обучающийся сделал не уверенный доклад по ВКР, но дал правильные и полные ответы не менее чем на 85 % заданных вопросов или обучающийся сделал уверенный доклад по ВКР, но дал правильные и полные ответы более чем на 75 %, но не более чем на 85 % заданных вопросов – 75…84 балла;
- обучающийся сделал не уверенный доклад по ВКР, но дал правильные и полные ответы более чем на 75 %, но не более чем на 85 % заданных вопросов или обучающийся сделал уверенный доклад по ВКР, но дал правильные и полные ответы более чем на 60 %, но не более чем на 75 % заданных вопросов – 60…74 балла;
- в прочих случаях – 0…59 баллов.

Шкала оценивания:

Количество баллов	0…59	60…74	75…84	85…100
Шкала	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично

оценивания				

Примерами таких вопросов являются:

1. В чем глобальные проблемы современности?
2. Основные признаки социальной философии
3. Какие были предпосылки образования Древнерусского государства?
4. Отличительные черты средневековья
5. Какой установлен порядок создания и регистрации деятельности хозяйствующих субъектов?
6. Перечислите виды основных фондов
7. Обозначьте критерии дифференциации гражданской дееспособности
8. Приведите пример правового отношения
9. Сделайте комплемент своему коллеге на русском и иностранном языке
10. Какие психологические барьеры возникают в общении?
11. Вы выяснили, что в Вашем коллективе два человека психологически не совместимы. Что вы предложите руководству? А как бы вы поступили, если бы были руководителем?
12. Что является основным специфическим средством формирования физической культуры личности?
13. Что такое здоровый образ жизни и здоровьесберегающие технологии?
14. Перечислите мероприятия по улучшению условий труда и снижению уровня производственного травматизма
15. Что необходимо сделать, если у человека произошел солнечный удар?
16. Правила при задании имени файла в командной строке
17. Что такое система управления базой данных?
18. Что такое планировщик ОС и какие имеются алгоритмы планирования? Как реализован планировщик в Windows и UNIX-системах?
19. Что такое изоляция приложений и методы ее обеспечения?
20. Что такое взаимная блокировка (dead-lock) и как ее избежать?
21. То такое инверсия приоритетов и как ее предотвратить,
22. Какие API синхронизации имеются в Windows?
23. Различие между параллельной н распределенной системами
24. Какие мотивации привели к созданию распределенных систем?
25. Масштабируемое приложение и способы достижения масштабируемости
26. Понятие прозрачности, формы прозрачности
27. Открытая система, ее преимущества
28. Концепции аппаратных решений, существующие для построения распределенных систем
29. Концепции программных решений, существующие хтя построения распределенных систем
30. Преимущества и недостатки распределенных систем
31. Понятие межуровневого интерфейса?
32. Что такое протокол?
33. Модель OSL ее уровни и их назначение.
34. Что такое удаленный вызов процедур, заглушки? Опишите по шагам пропесс удаленного вызова. Какие существуют расширенные модели RPC?
35. Обращение к удаленному объекту. Разница между статическим и динамическим обращением к объекту?
36. Что такое сохранность?
37. В чем отличие явной и неявной привязки ссылок на объект?
38. Типы связей, существующие в распределенных системах и их примеры
39. Требования, предъявляемые программистом к современным ОС?
40. Какие стандартные API имеются в современных ОС?
41. Что такое многозадачность и какие имеются разновидности.

42. Понятие многопоточности
43. Что такое планировшик ОС и какие имеются алгоритмы плани-рования? Как реализован планировщик в Windows и UNIX-системах?
44. Изоляция приложений и методы ее обеспечения
45. Что такое взаимная блокировка (dead-lock) и как ее избежать?
46. Что такое инверсия приоритетов и как ее предотвратить,
47. Какие API синхронизации имеются в Windows?
48. Какие API синхронизации имеются в UNIX?
49. Механизмы обмена данными между процессами?
50. Для чего необходимо управление правами доступа? Какие основные пели и средства описаны в (критериях определения безопасности компьютерных систем»?
51. Принцип мандатного управления доступом
52. Принцип избирательного (дискреционного) управления доступом
53. Какие средства сетевого взаимодействия существуют в современных ОС?
54. Почему необходимо синхронизировать время в распределенной системе? Приведите пример.
55. Понятие логического времени.
56. Что такое глобальное состояние н алгоритм получения распределенного снимка состояния?
57. Алгоритмы голосования: алгоритм забияки и кольцевой алгоритм.
58. Алгоритмы взаимного исключения: централизованный нераспрелеленный алгоритмы, алгоритм маркерного кольца.
59. Перечислите этапы развития реляционных СУБД и лайте определение основным понятиям теории реляционных БД.
60. В чем заключается целостность базы данных, перечислите операции реляционной алгебры?
61. Модель сервера БД (DBS).
62. Модель сервера приложений (AS).
63. Эволюция серверов БД.
64. Состав задач активного сервера.
65. Аспекты сетевого взаимодействия в распределенных системах.
66. Принципы взаимодействия «клиент-сервер».
67. Опишите технологию распределения и тиражирования данных. Приведите пример гетерогенной системы.
68. Технологии обработки данных в распределенной среде.
69. Что такое транзакция и в чем состоит принцип ACID? Какие примитивы транзакций вы знаете? Что такое вложенные транзакции и их особенность?
70. Как реализуются распределенные транзакции? Менеджеры транзакций.
71. Для чего используется журнал транзакций. Опишите механизм отката транзакций.
72. Механизм распределенных транзакций.
73. Как организован одновременный доступ к данным. Опишите механизм блокировок.
74. В чем стоит принцип двухфазной блокировки? В чем отличие реализации централизованной и распределенной двухфазной блокировки?
75. Понятие оптимистичной блокировки
76. Основные правила изучения научной литературы
77. Что такое рубрикация научной работы?
78. Перечислите основные методы проведения научных исследований

4. Рекомендации обучающимся по подготовке к процедуре защиты выпускной квалификационной работы

Подготовка к процедуре защиты выпускной квалификационной работы (ВКР) осуществляется следующим образом:

1. Обучающийся должен представить заведующему кафедрой полностью выполненную и сшитую ВКР установленного объема и оформленную в соответствии с установленными требованиями со всеми необходимыми подписями (обучающегося, руководителя, консультантов) в печатном и электронном варианте.

2. Заведующий кафедрой проверяет по формальным признакам (общий объем, структура, оформление, наличие всех необходимых подписей) соответствие ВКР установленным требованиям. Если ВКР хотя бы по одному формальному признаку не соответствует установленным требованиям, то обучающемуся предоставляется семь календарных дней для устранения выявленных не соответствий. Если по истечении семи календарных дней выявленные не соответствия устранены не будут, то обучающийся до защиты ВКР не допускается.

3. При соблюдении всех формальных признаков заведующий кафедрой электронный вариант ВКР передает ответственному лицу кафедры для проверки на долю заимствований, а также поручает руководителю ВКР подготовить отзыв на ВКР. В течение семи календарных дней ответственное лицо подготавливает справку на долю заимствований, а руководитель – отзыв на ВКР. Подготовленные справка на долю заимствований и отзыв на ВКР передаются заведующему кафедрой, который ознакомившись с ними, передает их обучающемуся вместе с подписанным печатным вариантом ВКР не менее чем за пять календарных дней до даты защиты ВКР.

4. Обучающийся знакомится со справкой на долю заимствований и отзывом, на обратной стороне жесткого переплета пояснительной записки формирует карман, в который вкладывает справку на долю заимствований и отзыв на ВКР, подписывается пояснительную записку ВКР у директора ИИТМА, после чего процедура допуска к защите завершается и обучающийся считается допущенным к защите ВКР. ВКР представляется на кафедру за день до даты защиты.

5 Примерные темы выпускных квалификационных работ (ВКР)

Тему ВКР обучающийся в обязательном порядке согласовывает с руководителем. Возможными темами ВКР являются:

1. Разработка систем защиты информации автоматизированных систем.
2. Формирование требований к защите информации в автоматизированных системах.
3. Тестирование систем защиты информации автоматизированных систем.
4. Разработка проектных решений по защите информации в автоматизированных системах.
5. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем.
6. Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем.
7. Обоснование необходимости защиты информации в автоматизированной системе.
8. Определение угроз безопасности информации, обрабатываемой автоматизированной системой.
9. Разработка архитектуры системы защиты информации автоматизированной системы.
10. Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.
11. Обеспечение информационной безопасности …..

12. Организация работы службы безопасности ….. .
13. Разработка пакета документов, необходимых для получения лицензии на деятельность по технической защите конфиденциальной информации.
14. Резервирование данных в условиях работы в распределенной сети. 5
15. Противодействие инсайдерской атакам на информационную систему организации …...
16. Оценка стоимости информационных активов предприятия …...
17. Защита конфиденциальной информации на мобильных устройствах.
18. Разработка системы мероприятий по защите от утечки информации по каналам …...
19. Организация защищенного внутреннего документооборота …...
20. Технические аспекты защиты интеллектуальной собственности …..
21. Организация безопасного обмена данными центрального офиса компании с филиалами …...
22. Разработка комплекса мероприятий, направленных на уменьшение вероятность реализации угроз информационной безопасности …...
23. Разработка автоматизированной системы контроля доступа в помещение.
24. Разработка политики безопасности в коммерческом предприятии.
25. Проблемы безопасности информационной системы банков и методы их преодоления.
26. Разработка системы защиты конфиденциальной информации.
27. Разработка системы защиты персональных данных коммерческого предприятия.
28. Сравнительный анализ средств защиты от НСД.
29. Организация защищенного электронного документооборота в организации.
30. Криптоанализ современных блочных и поточных шифров
31. Анализ эффективности различных методов биометрической аутентификации личности.
32. Техническая защита информационных систем персональных данных.
33. Реализация криптографической защиты информации в организации.
34. Разработка системы обнаружения вторжений в организации.
35. Разработка и защита базы данных организации. 2
36. Повышение эффективности защиты информации в ЛВС организации.
37. Разработка системы защиты речевой конфиденциальной информации в кабинете главного бухгалтера организации
38. Разработка системы защиты информационной системы персональных данных организации.
39. Разработка системы контроля и управления доступом …..
40. Разработка системы видеонаблюдения …...
41. Организация работы службы безопасности …...
42. Сравнительный анализ средств защиты от несанкционированного доступа.

10.05.03.07.Б1-2021-ФОС

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»
Институт информационных технологий, машиностроения и автотранспорта

Фонд оценочных средств итоговой (государственной итоговой) аттестации

Специальность 10.05.03 Информационная безопасность автоматизированных систем
Специализация «Анализ безопасности информационных систем»

Присваиваемая квалификация
"Специалист по защите информации"

Блок 3 «Государственная итоговая аттестация»
«Подготовка к процедуре защиты и защита выпускной квалификационной работы»

Формы обучения
Очная

Кемерово 2021

Фонд оценочных средств составили

Заведующий кафедрой	Информацинная безопасность		Е.В. Прокопенко

Фонд оценочных средств обсужден на заседании кафедры Информацинная безопасность

Протокол № 6 от 01.03.2021

Зав. кафедрой Информацинная безопасность  Е.В. Прокопенко

Согласовано учебно-методической комиссией по специальности 10.05.03 Информационная безопасность автоматизированных систем

Протокол № 6 от 01.03.2021

Председатель учебно-методической комиссии специальности 10.05.03 Информационная безопасность автоматизированных систем  Е.В. Прокопенко

подпись

Оглавление

1 Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы

В результате освоения образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем Специализация «Анализ безопасности информационных систем» у обучающихся должны быть сформированы следующие компетенции:

Наименование категории (группы) компетенций	Код и наименование компетенции выпускника
Универсальные компетенции	
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	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
Безопасность жизнедеятельности	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
Экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к коррупционному поведению
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 назначений, 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
Общепрофессиональные компетенции, соответствующие выбранной специализации программы специалитета	
ОПК-7.1	Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем
ОПК-7.2	Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации
ОПК-7.3	Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем
Профессиональные компетенции	

Тип задач - контрольно-аналитический	
ПК-1	Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-2	Способен выявлять уязвимости информационно-технологических ресурсов автоматизированных систем
ПК-3	Способен выявлять основные угрозы безопасности информации в автоматизированных системах
ПК-4	Способен определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем
ПК-5	Способен определять оценки возможностей реализации угрозы внешних и внутренних нарушителей
ПК-6	Способен анализировать характер обрабатываемой информации и определять перечень информации, подлежащей защите
ПК-7	Способен определять требуемый класс (уровень) защищенности автоматизированной системы
Тип задач - организационно-управленческий	
ПК-8	Выявляет степень участия персонала в обработке защищаемой информации
ПК-9	Способен составлять протоколы тестирования систем защиты информации автоматизированных систем
ПК-10	Способен планировать мероприятия по обеспечению защиты информации в автоматизированной системе
Тип задач - проектный	
ПК-11	Способен составлять методики и подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем
ПК-12	Способен обосновывать необходимость использования криптографических средств защиты информации
ПК-13	Способен разрабатывать отчетные документы и разделы технических заданий на создание систем защиты информации автоматизированных систем
ПК-14	Способен разрабатывать системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов
ПК-15	Способен разрабатывать модели угроз безопасности информации автоматизированной системы

2. Описание индикаторов достижения компетенций (показателей и критериев оценивания компетенций), используемых для оценивания результатов обучения при освоения образовательной программы

Код и содержание компетенции	Индикаторы достижения компетенции	Результаты обучения
Общепрофессиональные компетенции(ОПК)		
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	Оценивает роль информации, информационных технологий и информационной безопасности в современном обществе. Оценивает роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства. Владеет основами информационной безопасности, способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе Способен оценивать историю и элементы теории информационной культуры в современном обществе. Оценивает роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.	Знать объекты и виды профессиональной деятельности, состав задач, к решению которых должен быть подготовлен специалист, состав и назначение дисциплин образовательной программы; Знать основы новых информационных технологий переработки информации и их влияние на успех в профессиональной деятельности. Знать сущность и понятие информационной безопасности, характеристику ее составляющих; основные угрозы безопасности информации; место информационной безопасности в системе национальной безопасности страны. Знать историю и теорию информационной культуры. Знать значение и роль информации, информационных технологий для обеспечения объективных потребностей личности, общества и государства. Иметь опыт сбора, обработки и анализа информации для использования в профессиональной деятельности. Уметь использовать в образовательном процессе литературу и методические материалы по специальности, организовывать самостоятельную подготовку по учебным дисциплинам. Уметь работать в условиях возможного заражения ЭВМ вирусами; – уметь работать с программными средствами общего назначения, соответствующими современным требованиям мирового ранка программных средств. Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. Уметь применять информационные технологии для поиска и обработки информации. Уметь анализировать информацию и информационные технологии с точки зрения информационной безопасности для современного общества. Уметь оценивать роль информации, информационных технологий и информационной безопасности в профессиональной деятельности. Владеть навыками поиска учебной литературы и методических материалов по специальности. Владеть навыками поиска информации, необходимой для решения поставленной задачи. Владеть профессиональной терминологией.

		Владеть навыками использования информации, информационных технологий с учетом требования информационной безопасности в современном обществе Владеть навыками работы с современными информационными технологиями сбора, обработки и анализа.
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	Знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения. Ознакомлен со средства криптографической защиты информации при решении задач профессиональной деятельности.	Знать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. Иметь опыт определения назначения и принципов использования средств криптографической защиты информации. Умеет применять математические модели для оценки стойкости СКЗИ, использовать СКЗИ в автоматизированных системах. Уметь переделять назначение конкретных средства криптографической защиты информации. Владеть методами криптоанализа простейших шифров. Владеть навыками использования средств криптографической защиты информации.
ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем	Разрабатывает компоненты систем защиты информации автоматизированных систем Ознакомлен и владеет принципами создания компонент систем защиты информации автоматизированных систем.	Знать понятие, сущность, цели и задачи комплексной системы защиты информации – комплексной защиты информации, принципы организации и этапы разработки комплексной системы защиты информации; факторы, влияющие на организацию системы защиты информации; технологию определения состава защищаемой информации и объектов защиты; методы моделирования, анализа и оценки угроз защищаемой информации; виды моделей, описывающих процессы защиты информации; содержание технологического и организационного построения системы защиты информации на предприятии; состав мероприятий и условия, обеспечивающие функционирование системы защиты информации на предприятии; порядок кадрового, материально-технического и нормативно-методического обеспечения защиты информации на предприятии; порядок организации планирования и контроля комплексной системы защиты информации на предприятии; методику анализа эффективности системы защиты информации; порядок организации аттестации объектом информатизации по требованиям безопасности информации. Иметь опыт подбора компонент систем защиты информации. Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; формировать комплекс мер по защите информации на предприятии и оценивать их эффективность на основе заданных требований по безопасности информации; разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации на предприятии. Уметь подбирать компоненты систем защиты информации автоматизированных систем.

		Владеть методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации; технологией разработки организационнофункциональной структуры и комплекса нормативно-методического обеспечения комплексной защиты информации на предприятии. Владеть первичного навыками конфигурирования комплекса компонент систем защиты информации.
ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	Применяет знания в области безопасности вычислительных сетей электронных вычислительных машин Применяет знания в области безопасности операционных систем Имеет представление о системе управления базами данных как об одной из основных составляющих эффективных систем автоматизированной обработки информации; о современных концепциях безопасности баз данных. Организует работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем. Способен применять элементарные знания в области безопасности вычислительных сетей, операционных систем и баз данных Применяет знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем. Применяет знания в области безопасности вычислительных	Знать средства и методы хранения и передачи информации; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений. Знать принципы построения и функционирования, примеры реализаций современных операционных систем; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows. Знать принципы построения, функционирования, архитектуру, примеры реализаций современных систем управления базами данных; последовательность и содержание этапов проектирования баз данных; средства обеспечения безопасности данных. Знать классы защищенности автоматизированных систем и ее составных частей. Знать источники угроз информационной безопасности и меры по их предотвращению; жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности. Иметь опыт применения знаний в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем. Знать современное состояние уровня и направлений развития компьютерной техники и программных средств. Знать способы кодирования информации; основные телекоммуникационные протоколы. Уметь применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов.

	сетей, операционных систем и баз данных при разработке автоматизированных систем. Применяет знания в области безопасности сетей и систем передачи информации	Уметь использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надежность защиты операционных систем; планировать политику безопасности операционных систем. Уметь создавать объекты базы данных; выполнять запросы к базе данных; разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; применять средства обеспечения безопасности данных. Уметь определять класс защищенности автоматизированных систем. Уметь применять основные правила и документы системы сертификации Российской Федерации; классифицировать основные угрозы безопасности информации. Уметь применять знания в области безопасности вычислительных сетей при разработке автоматизированных систем; применять знания в области эксплуатации и обеспечения безопасности операционных систем при разработке автоматизированных систем; применять знания в области проектирования, разработки и эксплуатации баз данных, обеспечения безопасности систем баз данных при разработке автоматизированных систем. Уметь уверенно работать в качестве пользователя на ЭВМ, самостоятельно обеспечивая подготовку к работе накопителей на гибких дисках, создание резервных копий данных и программ. Уметь применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем. Владеть навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений. Владеть профессиональной терминологией в области информационной безопасности; навыками работы с операционными системами семейств UNIX и Windows, восстановление операционных систем после сбоев; навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности; навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности. Владеть языковыми средствами взаимодействия с реляционными базами данных; навыками нормализовывать отношения при проектировании реляционной базы данных;

		навыками реализации политики безопасности баз данных. Владеть знаниями в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем. Владеть навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и объектов информатизации; методами защиты информации. Владеть навыками применения основных средств обеспечения безопасности вычислительных сетей; навыками использования функциональных возможностей, в том числе средств администрирования, операционных систем для решения задач профессиональной деятельности; навыками проектирования, разработки и эксплуатации баз данных; навыками применения средств обеспечения информационной безопасности и администрирования систем управления базами данных. Владеть основами знаниями в области безопасности вычислительных сетей, операционных систем и баз данных. Владеть навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	Организует и проводит диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем от утечки по техническим каналам. Ознакомлен и владеет принципами организации, диагностики и тестирования систем защиты информации автоматизированных систем, анализа уязвимостей систем защиты информации автоматизированных систем. Организует и проводит диагностику и тестирование систем защиты информации	Знать принципы и методы организационной зашиты информации; универсальные приемы исследования оптимизационных проблем при различной степени неопределенности условий. Иметь опыт участия в диагностике и тестировании систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем. Знать методы, средства, анализа защищенности ПО информационных систем Уметь пользоваться нормативными документами по защите информации; решать типовые прикладные физические задачи. Уметь подбирать инструментарий для диагностики и тестирования систем защиты информации автоматизированных систем. Уметь проводить диагностику и тестирование систем защиты информации, проводить анализ уязвимостей систем защиты информации автоматизированных систем. Владеть методами формирования требований но защите информации; методами расчета и инструментального контроля показателей технической защиты информации. Владеть первичными навыками анализа уязвимостей систем защиты информации автоматизированных систем. Владеть методами и средствами анализа защищенности и верификации программного обеспечения информационных систем.

	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	Разрабатывает, внедряет и эксплуатирует автоматизированные системы с учетом требований по защите информации, проводит подготовку исходных данных для технико-экономического обоснования проектных решений применяет методы расчета эффективности инвестиционных проектов Ознакомлен и владеет знаниями о разработке, внедрении и эксплуатации автоматизированных систем с учетом требований по защите информации. Решает инженерно-геометрические задачи графическими способами. Эксплуатирует системы контроля и управления доступом к объекту информатизации	Знать требования защищенности автоматизированных систем в условиях актуальных угроз безопасности информации и их условия эксплуатации. Знать экономические критерии оценки проектных решений; Иметь опыт эксплуатации автоматизированных систем с учетом требований по защите информации; подготовки исходных данных для технико-экономического обоснования проектных решений. Знать основные законы геометрического формирования, построения и взаимного пересечения моделей плоскости и пространства. Знать современные методы и технические средства СКУД и основные подходы к созданию таких средств. Уметь проводить диагностика программных и аппаратных средств автоматизированных систем. Уметь оценивать эффективность инвестиционных проектов Уметь осуществлять подготовку исходных данных для технико-экономического обоснования проектных решений. Уметь воспринимать оптимальное соотношение частей и целого на основе графических моделей, практически реализуемых в виде чертежей конкретных пространственных объектов. Уметь разрабатывать меры защиты от выявленных угроз информационной безопасности, выбирать и устанавливать технические средства СКУД и оценивать их эффективность. Владеть аппаратно-программными средствами диагностики и контроля функционирования отдельных элементов, узлов, блоков автоматизированных систем. Владеть навыками подготовки исходных данных для технико-экономического обоснования проектных решений Владеть современным программным обеспечением для разных этапов решения профессиональных задач. Владеть графическими способами решения позиционных и метрических задач пространственных объектов на чертежах, методами проецирования и изображения пространственных форм на плоскости проекций. Владеть навыками внедрение и эксплуатации современных технических и программных средств СКУД.

ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Осуществляет администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем от утечки по техническим каналам Осуществляет администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем Ознакомлен и владеет знаниями об администрировании и контроле функционирования средств и систем защиты информации автоматизированных систем. Осуществляет администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем. Проводит аттестацию объектов информатизации.	Знать технические каналы утечки информации; способы и средства зашиты информации от утечек по техническим каналам; возможности технических разведок. Знать базовые понятия и подходы к управлению информационной безопасностью; международные и российские стандарты по УИБ; политика и ресурсное обеспечение ИБ организации. Иметь опыт администрирования средств и систем защиты информации. Знать средства и меры защиты и верификации программного обеспечения информационных систем. Знать положение об участии в организации и сопровождении аттестации объектов информатизации, архитектуру защищённых систем, основные понятия информационной безопасности. Уметь анализировать и оценивать угрозы информационной безопасности объекта; применять нормативные документы по метрологии, стандартизации и сертификации па практике. Уметь анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ. Уметь подбирать средства администрирования и контроля функционирования средств и систем защиты информации, выбирать инструментарий мониторинга защищенности автоматизированных. систем. Уметь проводить анализ защиты и верификации программного обеспечения информационных систем. Уметь применять методику оценки уязвимости в информационных сетях оценки, разрабатывать политику информационной безопасности на аттестуемых объектах, применять современные методы и средства защиты информации в информационно-телекоммуникационных системах. Владеть методами технической защиты информации; навыками обеспечения безопасности информации с помощью типовых программных и технических средств. Владеть современными методами и средствами разработки процессов управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность. Владеть навыками контроля функционирования средств и систем защиты информации. Владеть методами обеспечения качества разработки. Владеть выполнять анализ корпоративных данных, методами разработки политики информационной безопасности на аттестуемых объектах, разрабатывать структуру распределения 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	Анализирует 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. Интерпретирует многообразие исторических этапов, процессов мировой и отечественной истории, адаптацию к новым историческим реалиям , изменениям в профессиональной и общественной деятельности	Иметь опыт анализа основных этапов и закономерностей исторического развития России. Знать основные этапы исторического развития мировой и отечественной истории, их характерные черты, законы и закономерности обуславливающие динамику исторических процессов Уметь формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории России. Уметь выявлять предпосылки исторических процессов и событий, причинно-следственные связи явлений и процессов, анализировать исторические источники Владеть принципами историзма и научной объективности как основой формирования собственной гражданской позиции и развития патриотизма. Владеть знаниями и особенностями исторического развития мировой цивилизации, необходимыми для формирования гражданской позиции, адаптации к новым историческим реалиям Знать основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире.
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	Использует программные средства системного и прикладного назначений отечественного производства. Применяет программные средства системного и прикладного назначений для решения задач профессиональной деятельности Ознакомлен и владеет навыками использования программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	Знать современные программные средства системного и прикладного назначений, в том числе отечественного производства при решении задач профессиональной деятельности. Знать программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности. Иметь опыт запуска, редварительной настройки и использования программных средств системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности. Уметь выбирать современные программные средства системного и прикладного назначений для решении задач профессиональной деятельности. Уметь применять типовые программные средства защиты информации. Уметь определять назначение программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности. Владеть программными средствами системного и прикладного назначений. Владеть навыками применения программных средства системного и прикладного назначений для решения задач профессиональной деятельности. Владеть навыками использования программными средствами системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	Выбирает метод решения поставленной задачи, анализирует полученный результат. Выбирает фундаментальные законы, описывающие изучаемый процесс или явление Анализирует задачу, рассматривает возможные варианты ее решения, оценивая их достоинства и недостатки. Владеет криптографической терминологией; методами крипто-анализа простейших шифров; современной научно-технической литературой в области криптографической защиты. Составляет математическую модель, описывающую изучаемый процесс или явление, выбор и обоснование граничных и начальных условий. Оценивает адекватность результатов моделирования, формулирует предложения по использованию математической модели для решения задач профессиональной деятельности. Использует математические методы, необходимые для решения задач профессиональной деятельности.	Знать основные понятия и алгоритмы решения Знать основные понятия и законы естественных наук, методы математического анализа и моделирования Знать основные понятия, методы и приемы теории вероятностей и математической статистики Знать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. Знать фундаментальные законы, описывающие изучаемый процесс или явление Иметь опыт применения математических методов для решения задач профессиональной деятельности. Уметь использовать математические методы для решения поставленных задач Уметь использовать математический аппарат для разработки математических моделей явлений, процессов и объектов при решении инженерных задач в профессиональной деятельности Уметь выполнять статистическую обработку результатов Уметь использовать основные математические методы, используемые в анализе типовых криптографических алгоритмов. Уметь составлять математическую модель, описывающую изучаемый процесс или явление, объяснять ее выбор Уметь определять необходимые математические методы для решения задач профессиональной деятельности. Владеть основными техниками математических расчетов Владеть способами применения методов математического анализа и моделирования для обоснования принятия решений в профессиональной деятельности Владеть навыками решения профессиональных задач с использованием методов математической статистики Владеть навыками оценки адекватности результатов моделирования, формулированием предложения по использованию математической модели для решения задач профессиональной деятельности Владеть математическими методами решения задач профессиональной деятельности.
ОПК-4 Способен анализировать физическую сущность	Анализирует физическую сущность явлений и процессов, лежащих в основе функционирования	Знать физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; формы и способы представления данных в персональном компьютере. Знать основные физические явления, законы и процессы, лежащие в основе

явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	микроэлектронной техники. Применяет основные физические законы и модели для решения задач профессиональной деятельности, лежащие в основе функционирования микроэлектронной техники. Использует эмпирические и аналитические методы анализа физической сущности явлений и процессов, лежащих в основе функционирования микроэлектронной техники. Применяет физические законы и модели элементов электроники и схемотехники при разработке программно-аппаратных компонентов защищенных автоматизированных систем. Анализирует физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.	функционирования микроэлектронной техники в рамках общей физики. Знать виды физических явлений и процессов и способы их представления. Электронику и схемотехнику, технологию, методы и языки программирования, технологии связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности. Иметь опыт применения основных физических законов и моделей для решения задач профессиональной деятельности. Уметь анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности. Уметь самостоятельно анализировать физические процессы, происходящие в различных физических устройствах микроэлектронной техники. А также применять имеющиеся физические модели для решения задач профессиональной деятельности. Уметь использовать математический аппарат для анализа данных физических явлений и процессов. 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. Уметь использовать физические законы, анализировать и применять модели явлений, процессов и объектов (включая схемы электронных устройств) при решении инженерных задач в профессиональной деятельности. Владеть методами анализа для оценки физической сущности явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели. Владеть современными методами и подходами при решение физических задач, связанных с измерением параметров в различных технических устройствах. Владеть практическими методами физических явлений и процессов. 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. Владеть основными методами теоретического и экспериментального исследования физических явлений и процессов, в том числе лежащих в основе микроэлектронной техники.

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Владеет перечнем нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	Знать основные понятия и проблемы защиты информации в современных условиях. Знать первичные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. Знать нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации отечественные и . европейские критерии безопасности информационных технологий. Знать основы российской правовой системы и законодательства, правового статуса личности, организации деятельности органов государственной власти Российский Федерации по защите информации; виды и степень ответственности за правонарушения и преступления в информационной сфере. Иметь опыт применения нормативно-правовых и методических документов, регламентирующих деятельность по защите информации. Уметь использовать нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации для анализа состав задач, к решению которых должен быть подготовлен специалист по защите информации. Уметь использовать нормативные правовые акты в профессиональной деятельности. Уметь применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; анализировать правовые акты и осуществлять правовую оценку информации. Уметь применять действующую нормативную базу, нормативные правовые акты, нормативные и методические документы для принятия правовых и организационных мер по защите информации; разрабатывать проекты нормативно-правовых актов и организационно-распорядительных документов, регламентирующих деятельность по защите информации. Владеть основными понятиями профессиональной терминологии по информационной безопасности. Владеть оценочными стандартами и техническими спецификациями. Владеть навыками поиска нормативной правовой информации. необходимой для профессиональной деятельности навыками работы с нормативными правовыми актами. Владеть методами поиска и анализа нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации.
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации	Организует защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами	Знать нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, регламентирующие защиту информации ограниченного доступа в автоматизированных системах. Знать характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ; основы организационного и правового

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	Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Организует 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 Организует 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.	обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. Иметь опыт организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми документами ФСБ, ФСТЭК РФ. Уметь использовать нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при решении профессиональных задач. Уметь определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; предпринимать необходимые меры по восстановлению нарушенных прав. Уметь разрабатывать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах. Владеть навыками принятия решения о необходимости защиты информации при решении профессиональных задач. Владеть навыками организации охраны объектов информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации на предприятии. Владеть способами применения действующей нормативной базы в области защиты информации ограниченного доступа в автоматизированных системах.

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	Знает основные положения и концепции в прикладного и системного программирования, современные языки программирования, технологии создания и эксплуатации программных продуктов и программных комплексов. Способен писать программный код для реализации готовых алгоритмов. Умеет писать программы для реализации различных структур данных. Ознакомлен и владеет принципами создания программ на языках общего назначения, знает методы и инструментальные средства программирования для решения профессиональных задач.	Знать современные технологии и методы программирования; показатели качества программного обеспечения; методологии и методы проектирования программного обеспечения; методы тестирования и отладки программного обеспечения; принципы организации документирования разработки, процесса сопровождения; основные структуры данных и способы их реализации на языке программирования; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности. Знать синтаксис основных языков программирования, методы работы с данными на выбранном языке программирования. Иметь опыт выбора инструментария программирования и способов организации программ. Уметь формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; планировать разработку сложного программного обеспечения; проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; проводить комплексное тестирование и отладку программных систем; проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; использовать известные методы программирования и возможности базового языка. Уметь реализовывать разработанный алгоритм на выбранном языке программирования; работать с данными. Уметь осуществлять обоснованный выбор инструментария программирования и способов организации программ. Владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; навыками разработки программной документации; навыками программирования с использованием эффективных реализаций структур данных и алгоритмов. Владеть методами написания программы для реализации различных структур данных. Владеть навыками подбора языка, методов и инструментальных средств программирования для решения профессиональных задач.

ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	Использует программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем Использует программные и программно-аппаратные средства испытания систем защиты информационных систем Ознакомлен и владеет навыками использования программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем. Применяет прикладное программное обеспечение для моделирования элементов информационных систем.	Знать современные методы моделирования и испытания систем защиты информационных систем. Знать программные и программно-аппаратные средства испытания систем защиты информационных систем. Иметь опыт запуска, редварительной настройки и использования программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем. Знать инструментарий и приемы работы в графическом редакторе. Уметь интерпретировать полученные результаты для решения задач проектирования и прогнозирования качества работы систем защиты информационных систем Уметь использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем. Уметь определять назначение программных и программно-аппаратных средств. Уметь выполнять графические моделирование и представление информации в графическом редакторе. Владеть программными и программно-аппаратными средствами средствами для моделирования и испытания систем защиты информационных систем Владеть навыками анализа состояния информационной безопасности на конкретном объекте защиты. Владеть навыками использования программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем. Владеть навыками компоновки и графического моделирования объектов информационных систем в графическом редакторе.
ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	Разрабатывает методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации. Разрабатывает методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации Разрабатывает методики и тесты для анализа	Знать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации. Знать порядок работы с персоналом по вопросам обеспечения защиты информации ограниченного доступа, проведения мероприятий по физической и технической защите конфиденциальной информации, организации службы безопасности предприятия; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях. Иметь опыт разработки методик и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации. Знать показатели и нормы защищенности ПО от несанкционированного доступа к информации.

	степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации. Разрабатывает методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации.	Уметь использовать методики и проводить тесты для анализа степени защищенности информационной системы, определять её соответствие нормативным требованиям по защите информации. Уметь разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; организовывать работы по проверке кандидатов на должность, текущую работу с персоналом \ю обеспечению информационной безопасности. Уметь разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации. Уметь анализировать степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации. Владеть знаниями документации Федеральной службы по техническому и экспортному контролю (ФСТЭК России) по защите информации. Владеть навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности. Владеть навыками и инструментами разработки методик и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации. Владеть средствами защиты и тестирования программного обеспечения информационных систем для анализа степени защищенности.
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем	Проводит анализ защищенности и верификацию программного обеспечения информационных систем Проводит анализ защищенности и верификацию программного обеспечения информационных систем.	Знать документацию, сопровождающую процесс верификации и тестирования. Иметь опыт анализа защищенности и верификации программного обеспечения информационных систем. Уметь проводить анализ защищенности и верификацию программного обеспечения информационных систем. Уметь проводить анализ защищенности и верификацию программного обеспечения информационных систем. Владеть методами анализа защищенности и верификацию программного обеспечения информационных систем. Владеть методами, навыками, инструментами проведения анализа защищенности и верификации программного обеспечения информационных систем.
ОПК-8 Способен применять методы научных исследований при	Способен готовить обзоры, аннотации, составлять рефераты, научные доклады, публикации, и библиографии по научно-	Знать алгоритмы обработки структур данных, статистику, методы компьютерного моделирования объектов профессиональной деятельности Иметь опыт применения методов научных исследований при проведении разработок в области защиты информации в автоматизированных системах.

проведении разработок в области защиты информации в автоматизированных системах	исследовательской работе с учетом требований информационной безопасности. Применяет методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах.	Уметь работать с информационными источниками, опыт научного поиска, создания научных текстов. Уметь применять методы и системы искусственного интеллекта при реализации практических разработок в области защиты информации в автоматизированных системах; формулировать задачи исследования, выбирать методы и средства их решения. Владеть навыками оформления научных публикаций в соответствие с требованиями научных конференций Владеть навыками решения научно-технических задач в области своей профессиональной деятельности.
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	Использует сети и системы передачи информации с учетом текущего состояния и тенденций развития при решении задач профессиональной деятельности Применяет знания в области технической защиты информации, применяет их в работе с техническими каналами утечки информации, знает возможности технических разведок, знает способы и средства защиты информации от утечки по техническим каналам. Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.	Знать эталонную модель взаимодействия открытых систем современные виды информационного взаимодействия и обслуживания общие принципы проектирования современных систем и сетей телекоммуникаций, включая мультисервисные сети связи. Знать технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам. Иметь опыт решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации. Уметь читать структурные и функциональные схемы систем и сетей связи; проводить анализ показателей качества сетей и систем связи. Уметь анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, пользоваться нормативными документами по защите информации. Уметь проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно- технических решений, реализованных при построении ЭВМ и систем; применять средства защиты от утечки по техническим каналам при решении задач профессиональной деятельности; определять требования по защите коммуникационной среды распределенной информационной системы. Владеть навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений. Владеть методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации. Владеть навыками реализации вычислительных процедур на микропрограммном уровне при решении задач профессиональной деятельности; методами проектирования и навыками

		эксплуатации систем и сетей передачи информации при решении задач профессиональной деятельности; навыками проектирования распределенных информационных систем, в том числе разработки приложений, реализующих параллельные вычисления.
Профессиональные компетенции(ПК)		
ПК-1 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	Анализирует структурные и функциональные схемы защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем Исследует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем.	Знать структурные и функциональные схемы защищенных автоматизированных информационных систем, перечень уязвимостей информационной безопасности автоматизированных систем. Знать структурные и функциональные схемы защищенных автоматизированных информационных систем, перечень уязвимостей информационной безопасности автоматизированных систем. Знать технические средства контроля эффективности мер защиты информации. Иметь опыт проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем. Исследования программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах. Иметь опыт исследования программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах. Уметь проводить анализ структурных и функциональных схем. Уметь проводить анализ структурных и функциональных схем. Уметь контролировать безотказное функционирование технических средств защиты информации. Уметь проводить анализ структурных и функциональных схем защищенной автоматизированной системы. Уметь проводить анализ структурных и функциональных схем защищенной автоматизированной системы. Владеть навыками определения потенциальных уязвимостей информационной безопасности автоматизированных систем. Владеть навыками определения потенциальных уязвимостей информационной безопасности автоматизированных систем. Владеть методами анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем. Владеть методикой анализа информационной инфраструктуры и безопасности информации

		автоматизированных систем.
ПК-10 Способен планировать мероприятия по обеспечению защиты информации в автоматизированной системе	Планирует мероприятия по обеспечению защиты информации в автоматизированной системе Планирует мероприятия по обеспечению защиты информации в автоматизированной системе Планирует мероприятия по обеспечению защиты информации в автоматизированной системе. Планирует мероприятия по обеспечению защиты информации в автоматизированной системе. Формирует перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы.	Знать перечень мероприятий по обеспечению защиты информации. Знать перечень мероприятий по обеспечению защиты информации. Знать принципы формирования политики информационной безопасности в автоматизированных системах. Иметь опыт планирования мероприятий по обеспечению защиты информации в автоматизированной системе. Иметь опыт формирования перечня мероприятий по предотвращению угроз безопасности информации автоматизированной системы. Уметь планировать мероприятия по обеспечению защиты информации в автоматизированной системе. Уметь планировать мероприятия по обеспечению защиты информации в автоматизированной системе. Уметь формировать политику информационной безопасности. Уметь формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы. Уметь формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы. Владеть информационными технологиями планирования. Владеть информационными технологиями планирования. Владеть процедурами, практическими методами и руководящими принципами в области . Владеть навыками планирования мероприятий по обеспечению защиты информации в автоматизированной системе. Владеть навыками планирования мероприятий по обеспечению защиты информации в автоматизированной системе.

ПК-11 Способен составлять методики и подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем	Подбирает инструментальные средства тестирования систем защиты информации. Составляет методики тестирования систем защиты информации. Составляет методики и подбирает инструментальные средства тестирования систем защиты информации автоматизированных Составляет методики и подбирает инструментальные средства тестирования систем защиты информации автоматизированных Составляет методики и подбирает инструментальные средства тестирования систем защиты информации. Выбирает инструментальные средства тестирования систем защиты информации автоматизированных систем. Подбирает инструментальные средства тестирования систем защиты информации.	Знать инструментальные средства тестирования систем защиты. Знать принцип организации и проведения внутреннего аудита информационной безопасности. Знать инструментальные средства тестирования систем защиты информации. Знать инструментальные средства тестирования систем защиты информации. Иметь опыт составления методик тестирования систем защиты информации автоматизированных систем. Иметь опыт подбора инструментальных средств тестирования систем защиты информации автоматизированных систем. Знать понятие ИС, ее основные свойства, требования, необходимость защиты. Уметь использовать инструментальные средства тестирования элементов информационных систем. Уметь формировать корректирующие меры на основе результатов тестирования защищенности сети предприятия. Уметь составлять методики и подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем. Уметь анализировать основные узлы и устройства современных автоматизированных систем. Уметь контролировать безотказное функционирование технических средств защиты информации. Уметь составлять методики и подбирать инструментальные средства тестирования систем защиты информации. Владеть инструментальными средствами тестирования систем защиты информации. Владеть методиками тестирования систем защиты информации. Владеть методиками инструментального тестирования систем защиты информации автоматизированных систем. Владеть методиками инструментального тестирования систем защиты информации автоматизированных систем. Владеть составлением методик тестирования систем защиты информации автоматизированных систем. Владеть подбором инструментальных средств тестирования систем защиты информации автоматизированных систем. Владеть навыками тестирования систем защиты информации автоматизированных систем.

ПК-12 Способен обосновывать необходимость использования криптографических средств защиты информации	Обосновывает необходимость использования криптографических средств защиты информации Обосновывает необходимость использования криптографических средств защиты информации Применяет основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. Обосновывает необходимость использования криптографических средств защиты информации.	Знать криптографические средства защиты информации. Знать криптографические средства защиты информации. Иметь опыт применения основных криптографических методов, алгоритмов, протоколов, используемых для защиты информации в автоматизированных системах. Иметь опыт обосновывать критерии эффективности функционирования защищенных автоматизированных систем. Уметь навыками использования криптографических средств защиты информации. Уметь навыками использования криптографических средств защиты информации. Уметь применять основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. Уметь обосновывать критерии эффективности функционирования защищенных автоматизированных систем. Владеть навыками обоснования необходимости использования криптографических средств защиты информации. Владеть навыками обоснования необходимости использования криптографических средств защиты информации. Владеть обоснованием критериев эффективности функционирования защищенных автоматизированных систем.
ПК-13 Способен разрабатывать отчетные документы и разделы технических заданий на создание систем защиты информации автоматизированных систем	Разрабатывает отчетные документы и разделы технических заданий на создание систем защиты информации автоматизированных систем Разрабатывает отчетные документы и разделы технических заданий на создание систем защиты информации автоматизированных систем Разрабатывает отчетную документацию и разделы технических заданий. Разрабатывает отчетные документы на создание систем защиты информации. Разрабатывает разделы технических заданий на создание систем защиты информации.	Знать перечень отчетных документов, этапы разработки и разделы технических заданий на создание систем защиты информации автоматизированных систем. Знать перечень отчетных документов, этапы разработки и разделы технических заданий на создание систем защиты информации автоматизированных систем. Знать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Иметь опыт разработки отчетных документов. Иметь опыт разработки разделов технических заданий. Уметь разрабатывать отчетные документы и разделы технических заданий на создание систем защиты информации. Уметь разрабатывать отчетные документы и разделы технических заданий на создание систем защиты информации. Уметь использовать методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Уметь разрабатывать отчетные документы. Уметь разрабатывать разделы технических заданий. Владеть технологиями обработки электронной документации. Владеть технологиями обработки электронной документации. Владеть документацией по защите информации.

		Владеть опытом разработки отчетных документов. Владеть опытом разработки разделов технических заданий.
ПК-14 Способен разрабатывать системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов	Разрабатывает системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов Разрабатывает системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов. Формирует разделы технических заданий и проектной документации на создание систем защиты информации автоматизированных систем.	Знать системы защиты, нормативно-правовые документов по защите информации. Знать особенности проектирования подсистем информационной безопасности. Иметь опыт разработки систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов. Иметь опыт формирования разделов технических заданий и проектной документации на создание систем защиты информации автоматизированных систем. Уметь разрабатывать системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов. Уметь разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах. Уметь организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем. Уметь применять математические модели при проектировании систем защиты информации автоматизированных систем. Владеть навыками разработки системы защиты информации автоматизированных систем. Владеть методологиями построения систем защиты информации. Владеть разработкой систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов. Владеть формирование разделов технических заданий на создание систем защиты информации автоматизированных систем.
ПК-15 Способен разрабатывать модели угроз безопасности информации автоматизированной системы	Разрабатывает модели угроз безопасности информации автоматизированной системы. Разрабатывает модели нарушителей автоматизированной системы.	Знать модели угроз безопасности информации. Знать модели угроз безопасности информации. Знать основы теории построения систем информационной безопасности. Иметь опыт разработки модели угроз безопасности информации в автоматизированных системах. Иметь опыт разработки модели нарушителей в автоматизированных системах. Уметь разрабатывать модели угроз безопасности информации автоматизированной системы. Уметь разрабатывать модели угроз безопасности информации автоматизированной системы. Уметь строить модели угроз, нарушителя, защищаемого объекта. Уметь разрабатывать модели угроз безопасности информации в автоматизированных системах. Уметь разрабатывать модели нарушителей в автоматизированных системах. Владеть способами автоматизированной разработки моделей угроз. Владеть методами оценки экономической эффективности систем информационной безопасности. Владеть методами разработки модели угроз безопасности информации в

		автоматизированных системах. Владеть методами уточнения модели нарушителей автоматизированной системы.
ПК-2 Способен выявлять уязвимости информационно-технологических ресурсов автоматизированных систем	Выявляет уязвимости информационнотехнологических ресурсов автоматизированных систем. Выявляет уязвимости информационнотехнологических ресурсов автоматизированных систем. Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем. Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем. Анализирует доступные информационные источники с целью выявления известных уязвимостей используемых в системе защиты информации.	Знать перечень потенциальных уязвимостей информационно-технологических ресурсов автоматизированных систем. Знать методы и средства обнаружения угроз безопасности информационных систем. Иметь опыт выявления уязвимости информационно-технологических ресурсов автоматизированных систем. Иметь опыт анализа доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств. Уметь использовать современные информационные технологии в профессиональной деятельности. Уметь использовать современные информационные технологии в профессиональной деятельности. Уметь использовать современные решения для обнаружения угроз безопасности информационных систем. Уметь выявлять уязвимости информационно-технологических ресурсов автоматизированных систем. Уметь проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств. Владеть методами выявления уязвимости информационно-технологических ресурсов автоматизированных систем.
ПК-3 Способен выявлять основные угрозы безопасности информации в автоматизированных системах	Выявляет основные угрозы безопасности информации в автоматизированных системах. Выявляет основные уязвимости в автоматизированных системах. Выявляет основные угрозы безопасности информации в автоматизированных системах.	Знать перечень угроз безопасности информации. Знать перечень угроз безопасности информации. Знать особенности защиты информации в автоматизированных системах управления технологическими процессами. Организационные меры по защите информации. Иметь опыт выявления известных уязвимостей безопасности информационных систем. Иметь опыт выявления основных угроз безопасности информационных систем. Уметь определять основные угрозы безопасности информации с использованием современных информационных технологии. Уметь анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации. Уметь выявлять известные уязвимости информационных систем. Уметь анализировать возможные угроз информационных систем. Владеть способами выявления основных угроз безопасности информации в автоматизированных системах. Владеть способами выявления основных угроз безопасности

		информации в автоматизированных системах. Владеть методами выявления основные угрозы безопасности информации. Владеть методами выявления уязвимостей безопасности информации в автоматизированных системах. Владеть методами выявления основных угроз безопасности информации в автоматизированных системах.
ПК-4 Способен определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем	Определяет комплекс мер правила, процедуры, практические приемы, руководящие принципы, методы, средства для защиты информации автоматизированных систем. Определяет комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем. Определяет комплекс мер, правила, процедуры, практические приемы, руководящие принципы, методы, средства для защиты информации. Определяет комплекс мер, правила, процедуры, практические приемы, руководящие принципы, методы, средства для защиты информации.	Знать перечень мер, правил, процедур, практических приемов, руководящих принципов, методы, средства для защиты информации автоматизированных систем. Знать способы реализации угроз безопасности в автоматизированных системах. Иметь опыт определения комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем. Иметь опыт определения комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем. Уметь определять комплекс мер, правила, процедуры, практические приемы, руководящие принципы, методы, средства для защиты информации автоматизированных систем. Уметь определять комплекс мер, правила, процедуры, практические приемы, руководящие принципы, методы, средства для защиты информации автоматизированных систем. Уметь выявлять известные уязвимости информационных систем. Уметь применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем. Уметь обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации. Владеть способами определения перечня мер, правила, процедуры, практические приемы, руководящие принципы, методы, средства для защиты информации с использованием современных информационных технологии. Владеть способами определения перечня мер, правила, процедуры, практические приемы, руководящие принципы, методы, средства для защиты информации с использованием современных информационных технологии. Владеть правилами, процедурами, практическими приемами, руководящими принципами, методами, средствами) для защиты информации автоматизированных систем.

		Владеть методами определения комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем. Владеть методами определения комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем.
ПК-5 Способен определять оценки возможностей реализации угрозы внешних и внутренних нарушителей	Определяет оценки возможностей реализации угрозы внешних и внутренних нарушителей. Определяет оценки возможностей внешних и внутренних нарушителей. Оценивает информационные риски в автоматизированных системах от действия внешних и внутренних нарушителей. Оценивает возможность реализации угрозы внешних и внутренних нарушителей.	Знать перечень угроз внешних и внутренних нарушителей. Знать перечень угроз внешних и внутренних нарушителей. Знать эталонную модель взаимодействия открытых систем. Знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах. Иметь опыт оценки информационных рисков в автоматизированных системах от действия внешних и внутренних нарушителей. Иметь опыт определения оценки возможностей внешних и внутренних нарушителей. Уметь использовать полученную информацию, при оценке возможностей реализации угрозы внешних и внутренних нарушителей. Уметь составлять перечень угроз. Уметь оценивать информационные риски в автоматизированных системах от действия внешних и внутренних нарушителей. Уметь оценивать информационные риски в автоматизированных системах от действия внешних и внутренних нарушителей. Владеть способами определения оценок возможностей реализации угрозы внешних и внутренних нарушителей. Владеть способами определения оценок возможностей реализации угрозы внешних и внутренних нарушителей. Владеть методами обнаружения информационных угроз. Владеть методами определения оценки возможностей внешних и внутренних нарушителей.

ПК-6 Способен анализировать характер обрабатываемой информации и определять перечень информации, подлежащей защите	Анализирует характер обрабатываемой информации и определят перечень информации, подлежащей защите. Анализирует и определяет перечень информации, подлежащей защите. Анализирует характер обрабатываемой информации. Определяет перечень информации, подлежащей защите. Анализирует обрабатываемую информацию и определяет перечень информации, подлежащей защите.	Знать перечень информации, подлежащей защите. Знать перечень информации, подлежащей защите. Знать особенности различных информационных систем и технологий, их состав и возможности по обработке информации, характер и перечень информации, подлежащей защите. Иметь опыт анализа характера обрабатываемой информации. Иметь опыт определения перечня информации, подлежащей защите. Знать понятие защищенности информационных систем, определение защищенной информационной системы. Уметь анализировать характер обрабатываемой информации. Уметь анализировать характер обрабатываемой информации. Уметь использовать технологии сбора, размещения, хранения, накопления, преобразования и передачи данных. Уметь анализировать характер обрабатываемой информации. Уметь определять перечень информации, подлежащей защите. Уметь выявлять уязвимости информационно-технологических ресурсов автоматизированных систем. Владеть способами анализа характера обрабатываемой информации и методами определения перечень информации, подлежащей защите. Владеть современными системными программными средствами, сетевыми технологиями, мультимедиа технологиями, методами и средствами интеллектуализации информационных систем используемых для анализа характера информации. Методами определения перечня информации, подлежащей защите. Владеть методами анализа характера обрабатываемой информации. Владеть методами определения перечня информации, подлежащей защите. Владеть методами анализа защищенных информационных систем.
ПК-7 Способен определять требуемый класс (уровень) защищенности автоматизированной системы	Определяет требуемый класс уровень защищенности автоматизированной системы.	Знать классы и уровни защищенности автоматизированной системы. Знать классы и уровни защищенности автоматизированной системы. Иметь опыт определения требуемого класса (уровня) защищенности автоматизированной системы. Иметь опыт определения требуемого класса (уровня) защищенности автоматизированной системы. Уметь определять требуемый класс и уровень защищенности автоматизированной системы. Уметь определять требуемый класса (уровень) защищенности автоматизированной системы. Уметь определять требуемый класса (уровень) защищенности автоматизированной системы. Владеть навыками разработки информационных системам. Владеть навыками разработки информационных системам. Владеть методами определения требуемого класса (уровня) защищенности

		автоматизированной системы. Владеть методами определения требуемого класса (уровня) защищенности автоматизированной системы.
ПК-8 Выявляет степень участия персонала в обработке защищаемой информации	Выявляет степень участия персонала в обработке защищаемой информации.	Знать основные принципы работы с коллективом. Иметь опыт выявления степени участия персонала в обработке защищаемой информации Иметь опыт выявления степени участия персонала в обработке защищаемой информации. Знать содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации. Уметь анализировать степень участия персонала в работе с информацией. Уметь анализировать степень участия персонала в работе с информацией. Уметь выявлять степень участия персонала в обработке защищаемой информации. Уметь выявлять степень участия персонала в обработке защищаемой информации. Уметь управлять человеческими ресурсами в сфере информационной безопасности. Владеть навыками работы с персоналом. Владеть навыками работы с персоналом. Владеть методами выявления степени участия персонала в обработке защищаемой информации. Владеть методами выявления степени участия персонала в обработке защищаемой информации. Владеть технологией управления человеческими ресурсами.
ПК-9 Способен составлять протоколы тестирования систем защиты информации автоматизированных систем	Использует инструментальные средства тестирования систем защиты информационных систем и формирует протоколы тестирования . Составляет протоколы тестирования систем защиты информации. Составляет протоколы тестирования систем защиты информации автоматизированных систем. Составляет протоколы тестирования систем защиты информации автоматизированных систем. Составляет протоколы тестирования систем защиты информации.	Знать корректирующие меры по обеспечению систем защиты информации в информационных систем. Знать корректирующие меры по обеспечению систем защиты информации в информационных систем. Знать способы и принципы составления протоколов тестирования систем защиты информации. Знать способы и принципы составления протоколов тестирования систем защиты информации. Иметь опыт составления протоколов тестирования систем защиты информации автоматизированных систем. Иметь опыт выбора инструментальных средств тестирования систем защиты информации автоматизированных систем. Уметь использовать инструментальные средства тестирования при испытаниях на соответствие требованиям по защите информации. Уметь составлять протоколы испытаний на соответствие требованиям по защите информации. Уметь протоколы тестирования систем защиты информации автоматизированных систем. Уметь протоколы тестирования систем защиты информации автоматизированных систем. Уметь составлять протоколы тестирования систем защиты информации автоматизированных систем. Уметь подбирать инструментальные средства тестирования систем защиты информации

	Выбирает инструментальные средства тестирования систем защиты информации.	автоматизированных систем. Владеть инструментальными средствами тестирования защиты информации в хоже проверки технологического процесса обработки и хранения защищаемой информации. Владеть методами тестирования систем защиты информации в ходе проверки технологического процесса обработки и хранения защищаемой информации. Владеть способами обработки и составления отчетных документов. Владеть способами обработки и составления отчетных документов. Владеть методами составления протоколов тестирования систем защиты информации автоматизированных систем. Владеть методами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем.
Универсальные компетенции(УК)		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Анализирует задачу, выделяя ее базовые составляющие. Осуществляет поиск информации для решения поставленной задачи. Рассматривает возможные варианты решения задачи, оценивая их достоинства и недостатки Использует знание физических законов для решения поставленных задач.	Знать основные понятия и теоремы математики Знать основные законы механики, молекулярной физики и термодинамики, электростатики и электромагнетизма, волновой и квантовой оптики, ядерной физики и элементарных частиц; физический смысл и математическое изображение основных физических законов. Уметь работать со справочной литературой; применять полученные знания в области математики для решения поставленных задач Уметь самостоятельно анализировать физические явления, происходящие в природе и различных устройствах; самостоятельно работать со справочной литературой; выполнять необходимые расчеты и определять параметры процессов. Владеть основными техниками математических расчетов Владеть современными методами решения физических задач и измерения параметров различных процессов в технических устройствах и системах.
УК-10 Способен формировать нетерпимое отношение к коррупционному поведению	Имеет представление о морали и последствиях коррупционного поведения	Знать основные нормативно-правовые акты в сфере противодействия коррупции, последствия, к которым приводит коррупционное поведение для организации, государства и общества Уметь формировать нетерпимое отношение к коррупционному поведению Владеть навыками осуждения коррупционного поведения в рамках правового поля

УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Определяет круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. Определяет стратегию сотрудничества для достижения поставленной цели и взаимодействует с другими членами команды для решения задач	Знать основные информационные технологии, используемые в автоматизированных системах. Знать основы формулирования в рамках поставленной цели проекта совокупности задач, обеспечивающих ее достижение Уметь анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами. Уметь представлять поставленную задачу в виде конкретных заданий Владеть навыками составления плана-графика реализации проекта в целом и плана-контроля его выполнения. Владеть методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Использует коммуникативные навыки для построения максимально эффективного взаимодействия между членами рабочего коллектива	Знать основные приемы и нормы социального взаимодействия в процессе командной работы; технологии межличностной и групповой коммуникации Уметь устанавливать и поддерживать контакты, обеспечивающие успешную работу Владеть основными методами и приемами социального взаимодействия в команде
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Выполняет перевод профессиональных текстов с иностранного языка н а государственный язык РФ и с государственного языка РФ на иностранный Выбирает стиль общения и ведет деловую переписку н а государственном языке РФ и иностранном языке с учетом особенностей стилистики официальных и неофициальных писем и социокультурных различий в формате корреспонденции, в том числе устной коммуникации на	Знать читать и переводить общепрофессиональные и общенаучные тексты на иностранном языке; применять адекватные языковые средства для осуществления делового и межкультурного общения в профессиональной сфере. Знать принципы построения устного и письменного высказывания на русском языке; требования к деловой устной и письменной коммуникации. Уметь осуществлять устную коммуникацию в монологической и диалогической формах в ситуациях научного и профессионального обмена Уметь вести обмен деловой информацией в устной и письменной формах на русском языке. Владеть навыками языковой организации письменной и устной речи, применения на функциональном уровне правил межличностного и профессионального общения Владеть навыками создания письменных и устных текстов в деловой коммуникации на русском языке.

	русском и иностранном языках.	
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	Учитывает при социальном и профессиональном общении историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения Интерпретирует историю в контексте мирового исторического развития	Знать содержание категорий философии, а также основных философских учений о сущности и принципах развития общества; основные философские подходы к пониманию причин культурного разнообразия в обществе. Знать закономерности и особенности социально-исторического и этнического развития различных культур, ценностные основания межкультурного взаимодействия в контексте исторического знания. Уметь анализировать особенности развития различных культур в философском контексте; аргументировать и обосновывать суждения о необходимости сохранения межкультурного разнообразия в современном обществе. Уметь анализировать особенности развития различных культур в социально-историческом и этническом контексте; аргументировать и обосновывать суждения о необходимости сохранения межкультурного разнообразия в современном обществе. Владеть навыками применения научных методов познания мира; способностью соотносить особенности развития общества с культурными традициями, этическими и философскими установками. Владеть навыками толерантного общения в условиях межкультурного разнообразия общества, способностью формировать представление об окружающем мире и своём месте в нём, в соответствии с историческими и этнокультурными особенностями развития общества
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	Постоянно повышает уровень своей квалификации, занимается самообразованием Определяет и реализовывает приоритеты собственной деятельности и способы ее совершенствования.	Знать основные приемы эффективного управления собственным временем и профессиональным развитием; основные принципы саморазвития и самообразования на протяжении всей жизни Знать требования к профессионалам на рынке труда, нормативно-правовые документы регулирующие трудовое законодательство, основы предпринимательство с целью самореализации. Уметь эффективно планировать и контролировать собственное время; использовать методы саморегуляции, саморазвития и самообучения; планировать траекторию своего профессионального развития Уметь определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни. Владеть методами управления собственным временем и профессиональным развитием; технологиями приобретения, использования и обновления социокультурных и профессиональных знаний, умений и навыков; методиками саморазвития и самообразования в течение всей жизни

		Владеть современными технологиями для саморазвития и самопрезентации.
УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	Выбирает и применяет соответствующие своему физическому состоянию комплексы упражнений, регулирует интенсивность тренировок. Выбирает и применяет соответствующие своему физическому состоянию комплексы упражнений, регулирует интенсивность тренировок. Выбирает и применяет соответствующие своему физическому состоянию комплексы упражнений, регулирует интенсивность тренировок. Осуществляет здоровый образ жизни, укрепляет здоровье.	Знать основы здорового образа жизни, способы сохранения и укрепления здоровья, методы и средства физического воспитания. Знать основы здорового образа жизни, способы сохранения и укрепления здоровья, методы и средства физического воспитания. Знать основы здорового образа жизни, способы сохранения и укрепления здоровья, методы и средства физического воспитания. Знать значение физической культуры в формировании общей культуры личности, приобщении к общечеловеческим ценностям и здоровому образу жизни, профилактике вредных привычек. Уметь использовать средства физической культуры для развития двигательных умений и навыков; подбирать системы упражнений для воздействия на функциональные системы. Уметь использовать средства физической культуры для развития двигательных умений и навыков; подбирать системы упражнений для воздействия на функциональные системы. Уметь использовать средства физической культуры для развития двигательных умений и навыков; подбирать системы упражнений для воздействия на функциональные системы. Уметь интегрировать полученные знания в формирование профессионально значимых умений и навыков. Владеть методикой самоконтроля за состоянием своего организма во время самостоятельных занятий физической культурой; методами самостоятельного выбора физических упражнений для укрепления здоровья. Владеть методикой самоконтроля за состоянием своего организма во время самостоятельных занятий физической культурой; методами самостоятельного выбора физических упражнений для укрепления здоровья. Владеть методикой самоконтроля за состоянием своего организма во время самостоятельных занятий физической культурой; методами самостоятельного выбора физических упражнений для укрепления здоровья. Владеть методами и способами организации здорового образа жизни, способами сохранения и укрепления здоровья, методами и средствами физического воспитания, принципами построения физкультурно-оздоровительных занятий.
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности	Соблюдает в повседневной жизни и профессиональной деятельности правила, снижающие риск возникновения негативных событий, а также навыки поведения в условиях чрезвычайных ситуаций и военных конфликтов	Знать принципы обеспечения безопасности жизнедеятельности Уметь идентифицировать опасности, оценивать вероятность реализации потенциальной опасности в негативное событие, разрабатывать мероприятия по повышению уровня безопасности жизнедеятельности Владеть методами прогнозирования возникновения опасных или чрезвычайных ситуаций; навыками по применению основных методов защиты в условиях чрезвычайных ситуаций и военных конфликтов

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	Использует основные экономические теории и законы для анализа и прогнозирования принимаемых решений в повседневной жизни и профессиональной деятельности	Знать основные экономические категории, концепции, теории и законы Уметь использовать принципы экономического анализа процессов и тенденций Владеть навыками решения базовых экономических задач

3 Требования к выпускной квалификационной работе, порядку ее выполнения и порядку защиты

Выпускная квалификационная работа (ВКР) выполняется обучающимися самостоятельно в печатном виде и включает при необходимости комплект чертежей формата А1 (допускается для отдельных листов использования нестандартных форматов) и пояснительную записку на листах формата А4 (для отдельных листов допускается использование других форматов) объемом не менее 50 страниц.

На каждом листе графической части в правом нижнем углу должен быть установленной формы штамп (приложение А). По ходу работы соответствующие места в угловом штампе заполняются подписями обучающегося и руководителя.

Все чертежи должны иметь название, при этом размер букв по высоте не должен быть меньше 15 мм. Чертеж должен быть ясным, четким и равномерно заполненным. На каждом листе графической части общая незаполненная площадь должна составлять не более 15 % от общей площади листа. Каждый лист графической части должен иметь единый стиль оформления, а также порядковый номер в правом верхнем углу высотой шрифта не менее 20 мм.

Пояснительная записка – документ, содержащий систематизированные данные, обосновывающие, поясняющие и дополняющие все принятые решения в рамках ВКР, который, помимо текстовой части, должен сопровождаться иллюстрациями, диаграммами, схемами и т.д.

Пояснительная записка должна иметь следующую структуру:

- титульный лист;
- задание на выполнение ВКР;
- календарный план;
- аннотация;
- содержание;
- введение;
- основная часть (по теме ВКР);
- спецчасть (при необходимости);
- список литературы;
- приложения (при необходимости).

На титульном листе пояснительной записки должны быть подписи:

- заведующего кафедрой;
- руководителя ВКР;
- консультанта по нормоконтролю.

Объем и содержание ВКР должно соответствовать индивидуальному заданию, выданным руководителем ВКР после согласования его с заведующим кафедрой. Отклонения от задания возможны при их согласовании с руководителем ВКР.

Работа над ВКР ведется систематически с периодическим представлением результатов руководителю ВКР, а также консультантам для проверки. В ходе выполнения ВКР обучающийся консультируется с руководителем ВКР и консультантами, как при непосредственном взаимодействии, так и с использованием ресурсов ЭИОС КузГТУ, в том числе синхронного и (или) асинхронного взаимодействия посредством сети «Интернет». ВКР считается выполненной в полном объеме, если объем и содержание ВКР соответствует заданию (с учетом внесенных изменений и дополнений), на титульном листе пояснительной записки имеются подписи руководителя ВКР, а также консультантов по соответствующим разделам, листы графической части подписаны руководителем.

При защите ВКР обучающийся развешивает на специально подготовленных стендах листы графической части и выступает с докладом в течение 5-7 минут. В ходе доклада обучающийся располагается непосредственно у листов графической части и указкой показывает на те элементы, о которых он рассказывает. Зачитывать текст доклада не допускается. По окончании доклада обучающийся благодарит членов государственной экзаменационной комиссии за уделенное внимание и предлагает задать вопросы. Каждый член государственной экзаменационной комиссии задает до двух письменных и до двух устных вопросов, на которые обучающийся должен дать ответы. После дачи ответов на заданные вопросы процедура защиты ВКР для обучающегося считается законченной.

4 Критерии и шкала оценки результатов подготовки и защиты выпускной квалификационной работы

Во время защиты обучающемуся задаются вопросы, касающиеся темы ВКР, а также другие вопросы, позволяющие оценить сформированность заявленных компетенций.

Критерии оценивания результатов подготовки и защиты выпускной квалификационной работы (ВКР):

- обучающийся сделал уверенный доклад по ВКР, дал правильные и полные ответы более чем на 85 % заданных вопросов – 85…100 баллов;
- обучающийся сделал не уверенный доклад по ВКР, но дал правильные и полные ответы не менее чем на 85 % заданных вопросов или обучающийся сделал уверенный доклад по ВКР, но дал правильные и полные ответы более чем на 75 %, но не более чем на 85 % заданных вопросов – 75…84 балла;
- обучающийся сделал не уверенный доклад по ВКР, но дал правильные и полные ответы более чем на 75 %, но не более чем на 85 % заданных вопросов или обучающийся сделал уверенный доклад по ВКР, но дал правильные и полные ответы более чем на 60 %, но не более чем на 75 % заданных вопросов – 60…74 балла;
- в прочих случаях – 0…59 баллов.

Шкала оценивания:

Количество баллов	0…59	60…74	75…84	85…100
Шкала оценивания	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично

Примерами таких вопросов являются:

1. В чем глобальные проблемы современности?
2. Основные признаки социальной философии
3. Какие были предпосылки образования Древнерусского государства?
4. Отличительные черты средневековья
5. Какой установлен порядок создания и регистрации деятельности хозяйствующих субъектов?
6. Перечислите виды основных фондов
7. Обозначьте критерии дифференциации гражданской дееспособности
8. Приведите пример правового отношения
9. Сделайте комплемент своему коллеге на русском и иностранном языке
10. Какие психологические барьеры возникают в общении?
11. Вы выяснили, что в Вашем коллективе два человека психологически не совместимы. Что вы предложите руководству? А как бы вы поступили, если бы были руководителем?

12. Что является основным специфическим средством формирования физической культуры личности?
13. Что такое здоровый образ жизни и здоровьесберегающие технологии?
14. Перечислите мероприятия по улучшению условий труда и снижению уровня производственного травматизма
15. Что необходимо сделать, если у человека произошел солнечный удар?
16. Правила при задании имени файла в командной строке
17. Что такое система управления базой данных?
18. Что такое планировщик ОС и какие имеются алгоритмы планирования? Как реализован планировщик в Windows и UNIX-системах?
19. Что такое изоляция приложений и методы ее обеспечения?
20. Что такое взаимная блокировка (dead-lock) и как ее избежать?
21. То такое инверсия приоритетов и как ее предотвратить,
22. Какие API синхронизации имеются в Windows?
23. Различие между параллельной н распределенной системами
24. Какие мотивации привели к созданию распределенных систем?
25. Масштабируемое приложение и способы достижения масштабируемости
26. Понятие прозрачности, формы прозрачности
27. Открытая система, ее преимущества
28. Концепции аппаратных решений, существующие для построения распределенных систем
29. Концепции программных решений, существующие хтя построения распределенных систем
30. Преимущества и недостатки распределенных систем
31. Понятие межуровневого интерфейса?
32. Что такое протокол?
33. Модель OSL ее уровни и их назначение.
34. Что такое удаленный вызов процедур, заглушки? Опишите по шагам пропесс удаленного вызова. Какие существуют расширенные модели RPC?
35. Обращение к удаленному объекту. Разница между статическим и динамическим обращением к объекту?
36. Что такое сохранность?
37. В чем отличие явной и неявной привязки ссылок на объект?
38. Типы связей, существующие в распределенных системах и их примеры
39. Требования, предъявляемые программистом к современным ОС?
40. Какие стандартные API имеются в современных ОС?
41. Что такое многозадачность и какие имеются разновидности.
42. Понятие многопоточности
43. Что такое планировшик ОС и какие имеются алгоритмы плани-рования? Как реализован планировщик в Windows и UNIX-системах?
44. Изоляция приложений и методы ее обеспечения
45. Что такое взаимная блокировка (dead-lock) и как ее избежать?
46. Что такое инверсия приоритетов и как ее предотвратить,
47. Какие API синхронизации имеются в Windows?
48. Какие API синхронизации имеются в UNIX?
49. Механизмы обмена данными между процессами?
50. Для чего необходимо управление правами доступа? Какие основные пели и средства описаны в (критериях определения безопасности компьютерных систем»?
51. Принцип мандатного управления доступом
52. Принцип избирательного (дискреционного) управления доступом
53. Какие средства сетевого взаимодействия существуют в современных ОС?

54. Почему необходимо синхронизировать время в распределенной системе? Приведите пример.

55. Понятие логического времени.

56. Что такое глобальное состояние н алгоритм получения распределенного снимка состояния?

57. Алгоритмы голосования: алгоритм забияки и кольцевой алгоритм.

58. Алгоритмы взаимного исключения: централизованный нераспрелеленный алгоритмы, алгоритм маркерного кольца.

59. Перечислите этапы развития реляционных СУБД и лайте определение основным понятиям теории реляционных БД.

60. В чем заключается целостность базы данных, перечислите операции реляционной алгебры?

61. Модель сервера БД (DBS).

62. Модель сервера приложений (AS).

63. Эволюция серверов БД.

64. Состав задач активного сервера.

65. Аспекты сетевого взаимодействия в распределенных системах.

66. Принципы взаимодействия «клиент-сервер».

67. Опишите технологию распределения и тиражирования данных. Приведите пример гетерогенной системы.

68. Технологии обработки данных в распределенной среде.

69. Что такое транзакция и в чем состоит принцип ACID? Какие примитивы транзакций вы знаете? Что такое вложенные транзакции и их особенность?

70. Как реализуются распределенные транзакции? Менеджеры транзакций.

71. Для чего используется журнал транзакций. Опишите механизм отката транзакций.

72. Механизм распределенных транзакций.

73. Как организован одновременный доступ к данным. Опишите механизм блокировок.

74. В чем стоит принцип двухфазной блокировки? В чем отличие реализации централизованной и распределенной двухфазной блокировки?

75. Понятие оптимистичной блокировки

76. Основные правила изучения научной литературы

77. Что такое рубрикация научной работы?

78. Перечислите основные методы проведения научных исследований

5 Примерные темы выпускных квалификационных работ (ВКР)

Тему ВКР обучающийся в обязательном порядке согласовывает с руководителем. Возможными темами ВКР являются:

1. Разработка систем защиты информации автоматизированных систем.
2. Формирование требований к защите информации в автоматизированных системах.
3. Тестирование систем защиты информации автоматизированных систем.
4. Разработка проектных решений по защите информации в автоматизированных системах.
5. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем.
6. Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем.
7. Обоснование необходимости защиты информации в автоматизированной системе.

8. Определение угроз безопасности информации, обрабатываемой автоматизированной системой.

9. Разработка архитектуры системы защиты информации автоматизированной системы.

10. Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.

11. Обеспечение информационной безопасности …..

12. Организация работы службы безопасности ….. .

13. Разработка пакета документов, необходимых для получения лицензии на деятельность по технической защите конфиденциальной информации.

14. Резервирование данных в условиях работы в распределенной сети. 5

15. Противодействие инсайдерской атакам на информационную систему организации …...

16. Оценка стоимости информационных активов предприятия …...

17. Защита конфиденциальной информации на мобильных устройствах.

18. Разработка системы мероприятий по защите от утечки информации по каналам …...

19. Организация защищенного внутреннего документооборота …...

20. Технические аспекты защиты интеллектуальной собственности …..

21. Организация безопасного обмена данными центрального офиса компании с филиалами …...

22. Разработка комплекса мероприятий, направленных на уменьшение вероятность реализации угроз информационной безопасности …...

23. Разработка автоматизированной системы контроля доступа в помещение.

24. Разработка политики безопасности в коммерческом предприятии.

25. Проблемы безопасности информационной системы банков и методы их преодоления.

26. Разработка системы защиты конфиденциальной информации.

27. Разработка системы защиты персональных данных коммерческого предприятия.

28. Сравнительный анализ средств защиты от НСД.

29. Организация защищенного электронного документооборота в организации.

30. Криптоанализ современных блочных и поточных шифров

31. Анализ эффективности различных методов биометрической аутентификации личности.

32. Техническая защита информационных систем персональных данных.

33. Реализация криптографической защиты информации в организации.

34. Разработка системы обнаружения вторжений в организации.

35. Разработка и защита базы данных организации.

36. Повышение эффективности защиты информации в ЛВС организации.

37. Разработка системы защиты речевой конфиденциальной информации в кабинете главного бухгалтера организации

38. Разработка системы защиты информационной системы персональных данных организации.

39. Разработка системы контроля и управления доступом …..

40. Разработка системы видеонаблюдения …...

41. Организация работы службы безопасности …...

42. Сравнительный анализ средств защиты от несанкционированного доступа.