

Министерство науки и высшего образования РФ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»**

УТВЕРЖДЕНА
Ученым Советом
ПГНИУ

РЕКОМЕНДОВАНО
Кафедра процессов управления и
информационной безопасности

Протокол №10 от “25”

2017 г.

Протокол №4 от “13”

2017 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

по специальности: 10.05.01 Компьютерная безопасность
специализация: Разработка защищенного программного обеспечения
квалификация выпускника: Специалист
форма обучения: очная

Пермь 2017

Авторы-составители:

заведующий кафедрой к.т.н., доцент Кузнецов А.Г.,
доцент, к.ф.-м.н. Никитина Е.Ю.,
доцент, к.т.н. Черников А.В.

Содержание

| | |
|--|----|
| Введение..... | 4 |
| 1. Цель и задачи государственной итоговой аттестации | 4 |
| 2. Виды и объем государственной итоговой аттестации..... | 4 |
| 3. Результаты освоения образовательной (ОП) программы ВО..... | 5 |
| 3.1 Перечень общекультурных (ОК) компетенций, подтверждающих наличие у выпускника общих знаний и социального опыта..... | 5 |
| 3.2 Перечень общепрофессиональных (ОПК) компетенций и их индикаторов, на основе которых были освоены профессиональные компетенции (ПК)..... | 5 |
| 3.3 Перечень профессиональных (ПК) компетенций, владение которыми должен продemonстрировать обучающийся в ходе ГИА | 6 |
| 3.3.1 При сдаче государственного экзамена | 6 |
| 3.3.2 При защите выпускной квалификационной работы | 6 |
| 3.4 Перечень профессионально-специализированных (ПСК) компетенций, владение которыми должен продемонстрировать обучающийся в ходе ГИА..... | 7 |
| 4. Государственный экзамен..... | 8 |
| 4.1. Перечень вопросов государственного экзамена и примерное содержание ответов на них | 8 |
| 4.2 Критерии оценки результатов сдачи государственного экзамена..... | 29 |
| 4.2.1. Показатели и критерии оценивания компетенций | 29 |
| 4.2.1.1. Показатели и критерии оценивания ОК-компетенций | 29 |
| 4.2.1.2. Показатели и критерии оценивания ОПК-компетенций..... | 30 |
| 4.2.1.3. Показатели и критерии оценивания ПК-компетенций | 32 |
| 4.2.1.4. Показатели и критерии оценивания ПСК-компетенций..... | 35 |
| 4.2.2. Шкала и критерии оценки государственного экзамена | 36 |
| 4.3. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы с помощью государственного экзамена | 37 |
| 4.4. Учебно-методическое и информационное обеспечение государственного экзамена | 38 |
| 4.4.1. Список литературы | 38 |
| 4.4.2. Список нормативно-правовых документов..... | 41 |
| 4.4.3. Базы данных и информационно справочные системы..... | 44 |
| 5. Выпускная квалификационная работа | 46 |
| 5.1. Общая характеристика выпускной квалификационной работы..... | 46 |
| 5.2. Руководство и консультирование..... | 46 |
| 5.3. Требования к содержанию, объему, структуре и оформлению выпускной квалификационной работы..... | 47 |
| 5.4. Процедура защиты выпускной квалификационной работы | 49 |
| 5.5. Критерии оценки результатов защиты выпускной квалификационной работы..... | 51 |
| 5.5.1 Показатели и критерии оценки ОК-компетенций..... | 51 |
| 5.5.2. Показатели и критерии оценивания ОПК-компетенций | 54 |
| 5.5.3. Показатели и критерии оценивания ПК-компетенций | 57 |
| 5.5.4. Показатели и критерии оценивания ПСК-компетенций..... | 67 |
| 5.5.5. Шкала и критерии оценки защиты выпускной квалификационной работы | 70 |
| 6. Материально-техническое и программное обеспечение государственной итоговой аттестации | 73 |

Введение

Государственная итоговая аттестация (далее ГИА) – является обязательной и осуществляется после освоения образовательной программы высшего образования (ОП ВО) в полном объеме.

В соответствии с ОП ВО по специальности 10.05.01 Компьютерная безопасность деятельность ГИА включает следующие виды:

1. государственный экзамен в форме устных ответов на вопросы билетов государственного экзамена с обязательным письменным планом ответа на вопросы экзаменационного билета (форма выбирается самостоятельно);
2. защита выпускной квалификационной работы (ВКР) в форме устной защиты с раздаточным материалом и презентацией.

1. Цель и задачи государственной итоговой аттестации

Цель ГИА: установить уровень подготовки выпускника высшего учебного заведения к выполнению профессиональных задач в области информационной безопасности и соответствия его подготовки требованиям самостоятельного установленного образовательного стандарта высшего образования федерального государственного бюджетного образовательного учреждения высшего образования «Пермский государственный национальный исследовательский университет», утвержденный решением Ученого совета ПГНИУ Протокол № 10 от 25.06.2016 г. (далее – СУОС) по специальности 10.05.01 Компьютерная безопасность в области компетенций по видам профессиональной деятельности.

Задачи ГИА в соответствии с видами профессиональной деятельности, на которые ориентирована ОП ВО, охватывающие теоретические и практические аспекты будущей деятельности выпускника, оценить качество:

- 1) сформированности компетенций в практической, научно-исследовательской, контрольно-аналитической, эксплуатационной, организационно-управленческой деятельности;
- 2) подготовки выпускника к профессиональной деятельности и выполнению трудовых функций, соответствующих профессиональным стандартам и задачам.

2. Виды и объем государственной итоговой аттестации

ГИА включает государственный экзамен и защиту ВКР. Объем ГИА в соответствии с учебным планом – 6 з. е. (216 ак. часа), продолжительность 4 недели, из них 2 недели на подготовку и сдачу государственного экзамена, и 2 недели на подготовку и защиту выпускной квалификационной работы.

Государственный экзамен проводится по дисциплинам образовательной программы, результаты, освоения которых имеют определяющее значение для будущей профессиональной деятельности выпускников по специальности 10.05.01 Компьютерная безопасность.

3. Результаты освоения образовательной (ОП) программы ВО

3.1 Перечень общекультурных (ОК) компетенций, подтверждающих наличие у выпускника общих знаний и социального опыта

| | |
|-------|---|
| ОК-1 | владеть культурой мышления, способность использовать основы философских знаний для формирования мировоззренческой позиции, способность воспринимать, критически оценивать и обобщать новые знания |
| ОК-2 | владеть навыками коммуникации, уметь аргументировано и грамотно строить устную и письменную речь на русском языке, способность к общению в социальной и производственной деятельности |
| ОК-3 | способность работать самостоятельно и в коллективе, уметь находить и принимать организационно-управленческие решения, оценивать их эффективность |
| ОК-4 | критически анализировать и оценивать свой профессиональный и социальный опыт, при необходимости готовность изменить профиль своей профессиональной деятельности, демонстрировать готовность к саморазвитию и самосовершенствованию, повышению профессионального уровня и мастерства |
| ОК-5 | способность применять правовые и этические нормы в своей профессиональной деятельности и оценке ее последствий, знать свои права и способность занимать гражданскую позицию |
| ОК-6 | способность анализировать социально значимые проблемы и процессы |
| ОК-7 | знать и уважать историческое наследие и культурные традиции своей страны, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия, способность анализировать основные этапы и закономерности исторического развития общества |
| ОК-8 | владеть базовой лексикой и грамматикой одного из иностранных языков, основами разговорной речи; способность читать тексты на общеобразовательные и профессиональные темы, передавать их содержание на русском и иностранном языках |
| ОК-9 | владеть базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях, способность приобретать новые знания, используя современные информационные технологии |
| ОК-10 | понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны |
| ОК-11 | готовность пользоваться основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий |
| ОК-12 | понимать и стремиться соблюдать нормы здорового образа жизни, владеть средствами самостоятельного использования методов физического воспитания и укрепления здоровья |
| ОК-13 | способность использовать основы экономических знаний в различных сферах жизнедеятельности |

3.2 Перечень общепрофессиональных (ОПК) компетенций, на основе которых были освоены профессиональные компетенции (ПК)

| | |
|-------|---|
| ОПК-1 | способность использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с математическими и компьютерными науками |
| ОПК-2 | способность создавать, анализировать, реализовывать математические и информационные модели с применением современных вычислительных систем |
| ОПК-3 | способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности |
| ОПК-4 | готовность к участию в проведении научных исследований |
| ОПК-5 | способность действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма |
| ОПК-6 | способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства |

3.3 Перечень профессиональных (ПК) компетенций, владение которыми должен продемонстрировать обучающийся в ходе ГИА

3.3.1 При сдаче государственного экзамена

| | |
|-------|---|
| ПК-1 | способность взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий |
| ПК-3 | способность к анализу и формализации поставленных задач в области информационной безопасности |
| ПК-4 | способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности |
| ПК-6 | способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем |
| ПК-7 | способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований |
| ПК-11 | способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи |
| ПК-12 | способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований |
| ПК-22 | способность использовать нормативные правовые документы в своей профессиональной деятельности |
| ПК-23 | способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами |

3.3.2 При защите ВКР

| | |
|------|--|
| ПК-1 | способность взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий |
| ПК-2 | способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем |
| ПК-3 | способность к анализу и формализации поставленных задач в области информационной безопасности |
| ПК-4 | способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов области компьютерной безопасности |
| ПК-5 | способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций |
| ПК-6 | способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем |
| ПК-7 | способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований |
| ПК-8 | способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов |
| ПК-9 | способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем |

| | |
|-------|--|
| ПК-10 | способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах |
| ПК-12 | способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований |
| ПК-13 | способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей |
| ПК-14 | способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения |
| ПК-15 | способность оценивать эффективность системы защиты информации в компьютерных системах |
| ПК-16 | способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности |
| ПК-17 | способность разрабатывать планы работы первичных подразделений |
| ПК-18 | способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы |
| ПК-19 | способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем |
| ПК-20 | способность проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации |
| ПК-21 | способность принимать участие в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты информации |
| ПК-22 | способность использовать нормативные правовые документы в своей профессиональной деятельности |
| ПК-23 | способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами |

3.4 Перечень профессионально-специализированных (ПСК) компетенций, владение которыми должен продемонстрировать обучающийся в ходе ГИА

| | |
|-------|---|
| ПСК-1 | способность использовать современные методики и технологии программирования для разработки защищенного программного обеспечения |
| ПСК-2 | способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей |
| ПСК-3 | способность руководствоваться требованиями современных стандартов по безопасности компьютерных систем |
| ПСК-4 | способность проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов |
| ПСК-5 | способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах |
| ПСК-6 | способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности |

4. Государственный экзамен

4.1. Перечень вопросов государственного экзамена и примерное содержание ответов на них

Раздел «Математика»

Дисциплина «Алгебра и аналитическая геометрия»

1. Методы решения систем линейных уравнений
2. Конечно-мерные линейные пространства. Связь между базисами.
3. Китайская теорема об остатках. Приложения теории чисел.
4. Прямая и плоскость в пространстве: уравнения, условия взаимных расположений двух плоскостей, двух прямых, прямой и плоскости.
5. Линейное пространство геометрических векторов. Коллинеарные векторы. Компланарные векторы. Теорема о представлении любого вектора в виде линейной комбинации упорядоченной тройки некопланарных векторов
6. Введение аффинных координат на плоскости и в пространстве. Аффинные и метрические задачи на плоскости и в пространстве. Вывод различных уравнений плоскости в аффинной системе координат в пространстве.

Дисциплина «Теория вероятностей и математическая статистика I»

7. Аксиоматическое определение вероятности. Следствия из аксиом теории вероятностей.
8. Нормальное распределение. Его характеристики и свойства. Стандартное нормальное распределение. Сходимость по распределению. Асимптотическая нормальность. Центральная предельная теорема.
9. Точечное и доверительное оценивание параметрических функций. Методы получения точечных оценок для неизвестных параметров распределений: метод моментов, максимального правдоподобия, метод квантилей.

Дисциплина «Теория вероятностей и математическая статистика II»

10. Определение случайного вектора. Функция распределения случайного вектора, ее свойства. Частное распределение случайного вектора. Частная функция распределения случайного вектора. Связь между совместной и частной функцией распределения.
11. Свойства математического ожидания, дисперсии случайной величины. Свойства ковариационного момента случайных величин. Свойства коэффициента корреляции.
12. Вероятностная и статистическая модели случайного эксперимента. Основные типы статистических моделей: параметрическая, непараметрическая, байесовская, их достоинства и недостатки. Параметрическое и непараметрическое семейства распределений.

Дисциплина «Математический анализ I»

13. Понятие числовой последовательности, ее грани, арифметические операции. Бесконечно малые и бесконечно большие последовательности, их свойства.
14. Понятие функции, способы их задания, классификация. Предел функции в точке и на бесконечности. Бесконечно малые и бесконечно большие функции.
15. Функции нескольких переменных. Непрерывность. Дифференцирование. Экстремум функций двух переменных.
16. Определенный интеграл. Классы интегрируемых функций. Замена переменных в определенном интеграле.
17. Числовые и функциональные ряды. Необходимые и достаточные условия сходимости.
18. Степенные ряды. Абсолютная, условная и равномерная сходимость. Свойства равномерной сходимости рядов.

Дисциплина «Обыкновенные дифференциальные уравнения»

19. Дифференциальные уравнения первого порядка.

20. Дифференциальные уравнения второго порядка.

Дисциплина «Дискретная математика»

21. Экстремальные задачи теории графов: минимальное остовное дерево, кратчайший путь между вершинами, задача коммивояжера. Точные и приближенные алгоритмы для их решения: алгоритм Дейкстры, «жадные» алгоритмы.
22. Комбинаторные операции: сочетания и размещения (с возвратом и без возврата элементов). Комбинаторные принципы: сложение, умножение, дополнение, включение-исключение. Бином Ньютона. Полиномиальная формула.
23. Алфавитное кодирование: необходимое и достаточные условия однозначности декодирования. Теорема и алгоритм Маркова. Коды Хаффмана и Хэмминга.

Раздел «Программирование»

Дисциплина «Алгоритмизации и программирование I»

24. Работа с числами, превышающими возможности стандартных типов данных. Алгоритмы «длинной» арифметики.
25. Понятие структурного программирования. Принципы структурного программирования. Метод пошаговой детализации. Восходящее и нисходящее проектирование алгоритма.

Дисциплина «Теоретические основы информатики»

26. Сложность алгоритма. Оценка сложности нерекурсивных и рекурсивных алгоритмов. Понятие сложности задач. Классы сложности задач.
27. Алгоритмическая машина Поста. Машина Тьюринга. Нормальный алгоритм Маркова.

Дисциплина «Введение в компьютерные науки»

28. Понятие информационного процесса. Виды информационных процессов. Понятие информационных ресурсов, информационных систем. Эволюция информационных технологий. Классификация информационных систем.
29. Стандартные требования при производстве ЭВМ. Стандартные методики измерения производительности ЭВМ. Альтернативные методики измерения производительности ЭВМ.

Дисциплина «Методы и технологии программирования I»

30. Понятие сортировки. Параметры оценки алгоритмов сортировки. Классификация сортировок. Характеристики внутренних методов сортировки. Дополнительные факторы, учитываемые при сортировке. Хеширование. Рехеширование.
31. Понятие рекуррентных вычислений. Правила написания программ, содержащих рекуррентные вычисления.
32. Понятие рекурсии. Правила написания программ, содержащих рекурсивные вычисления.
33. Понятие алгоритмов с возвратами. Правила написания программ, содержащих алгоритмы с возвратами.

Дисциплина «Методы и технологии программирования II»

34. Понятие типа данных. Концепция типа данных. Пример характеристики типа данных.
35. Понятие дерева. Способы изображения деревьев. Способы представления деревьев. Обход дерева. Основные характеристики сбалансированных деревьев: идеально-сбалансированное дерево, АВЛ-дерево, красно-черное дерево, дерево случайного поиска, В-дерево.
36. Понятие графа. Способы изображения графов. Способы представления графов. Обход графа. Алгоритм нахождения кратчайшего пути в графе. Алгоритм нахождения множества достижимых вершин в графе.

37. Жизненный цикл программного обеспечения. Программы с большой и с малой жизнью. Этапы разработки программ по ГОСТ ЕСПД, по Майерсу. Технология макетирования. Модель водопада. Экстремальное программирование.
38. Принятие решений при разработке программ. Формальное обоснование принятых решений. Вариантные сектора, вариантная сеть.
39. Порядок сборки программы. Методы тестирования программ. Методы отладки программ.

Дисциплина «Языки программирования»

40. Особенности императивного программирования. Особенности функционального программирования. Функциональный стиль программирования. Области применения функционального программирования. Функциональное программирование на F#.
41. Особенности логического программирования. Области применения языка Пролог. Основы языка Пролог. Факты, правила, цель. Сопоставимость фактов.
42. Основные понятия объектно-ориентированного программирования. Принципы объектно-ориентированного программирования: инкапсуляция, наследование, полиморфизм. Исключения. Событийно-управляемое программирование.
43. Структура компилятора. Основные функции составных частей компилятора. Формальные и неформальные правила описания синтаксиса языка программирования.

Дисциплина «Базы данных и СУБД»

44. БД и СУБД. Основные функции СУБД. Многоуровневая архитектура современных СУБД.
45. Понятие модели данных (МД). Основные компоненты МД. Традиционные МД. Отличительные особенности семантических МД.
46. Понятие распределенных БД. Хранилища данных. Свойства хранилищ данных. Технологии хранилищ данных.
47. Жизненный цикл БД. Классификация и анализ рынка промышленных СУБД.

Дисциплина «Моделирование информационных систем»

48. Понятие модели информационной системы (ИС). Статическая, динамическая и функциональная модели ИС; связь между ними; относительная важность. Концептуальная модель, модель спецификации и модель реализации; различия в интерпретации. Понятие метамодели.
49. Язык UML, определение и назначение. Обзор основных диаграмм языка. Возможности их применения на различных этапах жизненного цикла информационной системы.

Раздел «Защита информации»

Дисциплина «Аппаратные средства вычислительной техники»

50. Процессоры компании Intel. Архитектура процессоров IA-32. Микроархитектура процессоров Intel.
51. Процессоры Intel в реальном режиме: регистры процессора, управление памятью и программами, данные и способы адресации, система команд, система прерываний.
52. Процессоры Intel в защищенном режиме: регистры процессора, управление памятью, поддержка многозадачности и защита памяти.
53. Архитектура ядра RISC микроконтроллера Atmel
54. Основы программирования микропроцессорных систем

Дисциплина «Основы информационной безопасности»

55. Информационная безопасность в системе национальной безопасности Российской Федерации. Система обеспечения информационной безопасности России.
56. Основные понятия информационной безопасности. (ФЗ «О безопасности», «Об информации, информационных технологиях и о защите информации», Стратегия национальной безопасности РФ, Доктрина информационной

безопасности РФ, ГОСТ Р 50922-2006; системный подход).
Общеметодологические принципы теории ИБ (общие понятия информационной безопасности, их взаимосвязь по ГОСТ Р ИСО/МЭК 15408, “Общие критерии”)).

57. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Понятия “менеджмента информационной безопасности”, “Политики информационной безопасности”.

Дисциплина «Организационно-правовое обеспечение защиты информации»

58. Четырехуровневая система как метод анализа информационной безопасности
59. Уголовно – правовая характеристика состава преступлений, предусмотренных ст.272-274 Уголовного кодекса РФ
60. Организация государственного контроля и надзора за соблюдением требований к защите информации в РФ

Дисциплина «Информационное право»

61. Классификация информации с точки зрения ФЗ «Об информации, информационных технологиях и о защите информации».
62. Информация как предмет частных правоотношений
63. Информация как предмет публичных правоотношений

Дисциплина «Российские и международные стандарты по защите информации»

64. Стандарт ISO 27000
65. Стандарт BSI (Германия). Федеральные критерии безопасности информационных технологий (США). Международный стандарт COBIT.
66. Общие требования по защите информации, предусмотренные РД, Приказом №17, Требованиями и Положениями ФСТЭК России, СТР-К
67. Общие нормативные требования по защите персональных данных

Дисциплина «Криптографические методы защиты информации»

68. Алгоритмы блочного шифрования. ГОСТ Р 34.12-2015
69. Алгоритмы шифрования с открытым ключом. Алгоритм RSA.
70. Криптографические хеш-функции. ГОСТ Р 34.11-2012
71. Электронная подпись. ГОСТ Р 34.10-2012
72. Режимы блочного шифрования ГОСТ Р 34.13-2015
73. Криптографический генератор псевдослучайных чисел

Дисциплина «Криптографические протоколы»

74. Протокол SSL.
75. Протокол Kerberos.
76. Протоколы аутентификации

Дисциплина «Компьютерные сети»

77. Сравнительная характеристика моделей OSI и TCP/IP
78. Протоколы модемной связи
79. Протоколы маршрутизации
80. Протоколы туннельной передачи данных

Дисциплина «Защита операционных систем»

81. Реализация системы защиты операционных систем семейства Microsoft Windows.
82. Реализация системы защиты UNIX-подобных операционных систем.
83. Управление процессами и потоками: представление процессов и потоков в операционных системах, дисциплины планирования процессов, взаимодействие процессов, проблема тупиков.
84. Управление оперативной памятью: управление физической и виртуальной памятью, реализация свопинга.
85. Управление файловыми системами: организация дискового пространства, современные файловые системы.

Дисциплина «Защита информационных систем от вредоносных программ»

86. Вредоносные программы: классификация, основные характеристики, современные тенденции в развитии вредоносных программ.

87. Компьютерные вирусы: классификация, основные характеристики, способы внедрения в программный код, способы сокрытия факта заражения и основные демаскирующие признаки
 88. Антивирусные программы: классификация антивирусных программ, способы обнаружения и уничтожения вредоносного кода, характеристика современных антивирусных программ.
- Дисциплина «Проектирование и разработка приложений в защищенном исполнении»
89. Угрозы информационной безопасности программного обеспечения. Модели безопасности информационных систем.
 90. Функциональные требования безопасности: методика формирования требований, реализация функциональных требований безопасности.
 91. Требования доверия к безопасности информационных систем: методика формирования требований, поддержание доверия к безопасности информационных систем и программных продуктов.
- Дисциплина «Технические средства и методы защиты информации»
92. Классификация технических каналов утечки информации
 93. Виды и источники носителей защищаемой информации.
 94. Виды контроля эффективности защиты информации
- Дисциплина «Противодействие техническим средствам разведки»
95. Оценка угроз акустических каналов утечки информации. Непреднамеренное прослушивание. Технические средства контроля звукоизоляции ограждающих конструкций.
 96. Порядок и методика аттестации защищаемых помещений.
 97. Порядок выявления специальных электронных устройств негласного перехвата информации в средствах вычислительной техники при подготовке к аттестации по требованиям безопасности информации.
- Дисциплина «Программно-аппаратные средства защиты информации»
98. Контроль целостности аппаратных, программных ресурсов и гарантированное уничтожение информации;
 99. Управление доступом. Дискреционный и мандатный методы доступа. Изолированная программная среда.
 100. Автоматизированные средства защиты информации от НСД
- Дисциплина «Защита баз данных»
101. Архитектурные особенности и транзакционные модели современных СУБД;
 102. Разграничение доступа в современных СУБД;
 103. Защита информации на уровне сервера
 104. Защита информации на уровне базы данных
 105. Администрирование современных СУБД. Обеспечения безопасности данных в современных СУБД на примере СУБД Oracle. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных.
 106. Администрирование современных СУБД. Обеспечения безопасности данных в современных СУБД на примере СУБД Firebird. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных
- Дисциплина «Защита компьютерных сетей»
107. Защита инфраструктуры маршрутизации
 108. Защита инфраструктуры коммутации
 109. Защита сетевой инфраструктуры
 110. Защита периметра сети
 111. Криптографическая защита каналов передачи данных
- Дисциплина «Психологические основы профессиональной деятельности»

112. Роль эффективных коммуникаций в информационной безопасности предприятия
113. Мотивация работника в структуре политики безопасности предприятия
114. Психологические методы ведения информационно-психологической войны.

Дисциплина «Психологические средства и методы защиты информации»

115. Роль организационной культуры в создании эффективной системы безопасности предприятия.
116. Способы и приемы безопасной кадровой политики на предприятии.
117. Роль групповой динамики в поддержании информационной безопасности предприятия

Дисциплина «Теоретико-числовые методы в криптографии»

118. Алгоритм RSA. Принцип работы, взаимная обратность отображений шифрования и дешифрования, вопросы выбора параметров, приложения, основные виды атак.
119. Методы факторизации натуральных чисел
120. Эллиптические кривые в криптографии.

Раздел 1. Математика

Тема 1. Методы решения систем линейных уравнений

Свойства решений системы линейных однородных уравнений. Доказательство, что множество всех решений СЛОУ является линейным пространством. Нахождение базиса и размерности линейного пространства. Связь общего решения СЛНУ и общее решение соответствующего СЛОУ.

Тема 2. Конечно-мерные линейные пространства. Связь между базисами.

Определение конечномерного линейного пространства. Определение базиса. Матрица перехода между двумя базисами.

Тема 3. Китайская теорема об остатках. Приложения теории чисел.

Китайская теорема об остатках: определение, доказательство. Приложения теории чисел. На примере криптографии.

Тема 4. Прямая и плоскость в пространстве: уравнения, условия взаимных расположений двух плоскостей, двух прямых, прямой и плоскости.

Определение прямой и плоскости в пространстве. Уравнения прямой и плоскости. Условия взаимных расположений двух плоскостей, двух прямых, прямой и плоскости.

Тема 5. Линейное пространство геометрических векторов. Коллинеарные векторы.

Компланарные векторы. Теорема о представлении любого вектора в виде линейной комбинации упорядоченной тройки некопланарных векторов

Понятия линейного пространства, геометрического вектора. Характеристики геометрических векторов. Операции над геометрическими векторами, их свойства. Коллинеарные и компланарные вектора, их свойства. Необходимые и достаточные условия коллинеарности двух векторов и компланарности трех векторов. Формулировка и доказательство теоремы о представлении любого вектора в виде линейной комбинации упорядоченной тройки некопланарных векторов.

Тема 6. Введение аффинных координат на плоскости и в пространстве. Аффинные и метрические задачи на плоскости и в пространстве. Вывод различных уравнений плоскости в аффинной системе координат в пространстве.

Определение прямоугольной декартовой и аффинной систем координат на плоскости и в пространстве. Аффинные и метрические задачи. Различные способы задания прямой в аффинной системе координат. Различные виды уравнений плоскости в аффинной системе координат в пространстве и их вывод.

Тема 7. Аксиоматическое определение вероятности. Следствия из аксиом теории вероятностей

Простейшие способы определения вероятности (классическое, геометрическое и статистическое). Алгебраические операции над событиями и их свойства, основные свойства вероятности. Основные аксиомы. Следствия из аксиом теории вероятности.

Тема 8. Нормальное распределение. Его характеристики и свойства. Стандартное нормальное распределение. Сходимость по распределению. Асимптотическая нормальность. Центральная предельная теорема

Определение, характеристики и свойства нормального распределения. Понятие стандартного нормального распределения: плотность и функция. Сходимость по распределению: определение, свойства, примеры. Асимптотическая нормальность: определения, свойства, примеры. Центральная предельная теорема: определение, доказательство, обобщения.

Тема 9. Точечное и доверительное оценивание параметрических функций. Методы получения точечных оценок для неизвестных параметров распределений: метод моментов, максимального правдоподобия, метод квантилей

Точечное и доверительное оценивание параметрических функций: определения, оценка, состоятельность, методы. Методы получения точечных оценок для неизвестных параметров распределения: метод моментов, максимального правдоподобия, метод квантилей – определения, оценка, сравнение, примеры.

Тема 10. Определение случайного вектора. Функция распределения случайного вектора, ее свойства. Частное распределение случайного вектора. Частная функция распределения случайного вектора. Связь между совместной и частной функцией распределения

Понятие случайного вектора. Понятие функции распределения случайного вектора. Свойства функции распределения случайного вектора. Частное распределение и частная функция распределения случайного вектора. Установление связи между совместной и частной функциями распределения случайного вектора.

Тема 11. Свойства математического ожидания, дисперсии случайной величины.

Свойства ковариационного момента случайных величин. Свойства коэффициента корреляции

Понятие случайной величины. Закон распределения вероятностей. Понятие математического ожидания, дисперсии, среднеквадратического отклонения, моды, медианы случайной величины, их свойства. Понятие ковариационного момента случайных величин, его свойства. Понятие коэффициента корреляции, его свойства. Корреляционная и ковариационная матрицы.

Тема 12. Вероятностная и статистическая модели случайного эксперимента. Основные типы статистических моделей: параметрическая, непараметрическая, байесовская, их достоинства и недостатки. Параметрическое и непараметрическое семейства распределений

Вероятностная и статистическая модели случайного эксперимента. Основные типы статистических моделей: параметрическая, непараметрическая, байесовская; достоинства и недостатки каждой из моделей. Параметрическое и непараметрическое семейство распределений. Основные виды статистического вывода: точечное и доверительное оценивание, проверка гипотез. Независимая повторная выборка как частный случай линейной модели наблюдений. Выборочное пространство. Сужение выборочного пространства. Достаточные статистики.

Тема 13. Понятие числовой последовательности, ее грани, арифметические операции.

Бесконечно малые и бесконечно большие последовательности, их свойства

Понятие последовательности и ее сходимости. Предел последовательности. Бесконечно малые и бесконечно большие последовательности. Ограниченные и неограниченные последовательности. Основные свойства сходящихся последовательностей. Сходимость монотонных последовательностей. Подпоследовательности. Предельные точки последовательности. Теорема Больцано-Вейерштрасса. Верхний и нижний пределы последовательности. Критерий Коши сходимости последовательности.

Тема 14. Понятие функции, способы их задания, классификация. Предел функции в точке и на бесконечности. Бесконечно малые и бесконечно большие функции

Определение функции. Определение предельного значения функции в точке. Односторонние пределы. Предел функции по базе. Бесконечно малые и бесконечно большие функции на бесконечности. Арифметические операции над функциями, имеющими предел. Замечательные пределы. Сравнение бесконечно малых и бесконечно больших функций. Критерий Коши существования предела функции.

Тема 15. Функции нескольких переменных. Непрерывность. Дифференцирование.

Экстремум функций двух переменных

Понятие n -мерного координатного и n -мерного векторного пространства. Топологические понятия n -мерного пространства: окрестность точки; открытые и замкнутые множества; предельные, граничные точки множества, точки прикосновения; связные множества, области. Сходимость последовательности точек, критерий Коши, теорема Больцано-Вейерштрасса. Предел функции n переменных в точке. Понятие предела по направлению, повторные пределы. Непрерывность функции n переменных. Свойства непрерывных функций на ограниченных замкнутых множествах.

Понятие частной производной. Два определения дифференцируемой функции в точке, их эквивалентность. Дифференцируемость и непрерывность. Необходимое условие дифференцируемости. Достаточное условие дифференцируемости. Непрерывно дифференцируемые функции. Дифференцирование сложной функции. Первый дифференциал, инвариантность его формы.

Понятие локального экстремума. Необходимое условие экстремума. Достаточное условие экстремума. Наибольшее и наименьшее значения функции. Условный экстремум.

Тема 16. Определенный интеграл. Классы интегрируемых функций. Замена переменных в определенном интеграле

Понятие определенного интеграла, сумма Римана. Суммы Дарбу и их свойства. Необходимое условие интегрируемости. Необходимое и достаточное условия существования определенного интеграла. Классы интегрируемых функций. Свойства определенного интеграла: арифметические операции над интегрируемыми функциями; свойства интеграла, выраженные неравенствами; теоремы о среднем. Свойства определенного интеграла с верхним переменным пределом, связь определенного интеграла с неопределенным. Основная формула интегрального исчисления. Замена переменной и интегрирование по частям в определенном интеграле.

Геометрические приложения определенного интеграла: вычисление длины дуги спрямляемой кривой, площади криволинейной трапеции и криволинейного сектора, вычисление объема тел вращения.

Тема 17. Числовые и функциональные ряды. Необходимые и достаточные условия сходимости

Числовой ряд и его сходимость. Критерий Коши. Основные свойства сходящихся рядов, необходимое условие сходимости. Критерий сходимости знакоположительного ряда. Признаки сравнения в простой и предельной форме. Признаки Даламбера, Коши, интегральный признак.

Абсолютная и условная сходимость знакопеременных рядов. Признак Лейбница. Признак Абеля-Дирихле.

Понятие функциональной последовательности и функционального ряда. Равномерная сходимость на множестве, критерий Коши равномерной сходимости. Достаточные признаки равномерной сходимости: признак Вейерштрасса, признак Абеля-Дирихле, признак Дини. Свойства равномерно сходящихся последовательностей и рядов: непрерывность суммы (предельной функции), почленное интегрирование и дифференцирование.

Тема 18. Степенные ряды. Абсолютная, условная и равномерная сходимость. Свойства равномерной сходимости рядов

Степенной ряд и область его сходимости, теорема Коши-Адамара. Функциональные свойства степенных рядов. Разложение функций в степенные ряды. Ряды Тейлора. Оценка погрешностей.

Ортогональные системы функций. Свойства периодических функций. Определение коэффициентов Фурье; случай четной и нечетной функций.

Разложение функций в ряд Фурье. Интеграл Дирихле. Основная лемма. Принцип локализации. Теорема о сходимости ряда Фурье в точке. Разложение функций, заданных на отрезке, в неполные ряды Фурье.

Тема 19. Дифференциальные уравнения первого порядка

Определение дифференциального уравнения. Понятие общего и частного решений. Поле направлений, изоклины. Уравнение с разделяющимися переменными. Однородные уравнения и уравнения, приводящиеся к однородным. Линейные уравнения первого порядка. Уравнение Бернулли. Уравнение Риккати. Уравнения в полных дифференциалах. Уравнения с интегрирующим множителем.

Тема 20. Дифференциальные уравнения n-го порядка

Понятие уравнения n-го порядка. Сведение к системам дифференциальных уравнений. Уравнения, допускающие понижение порядка и методы их решений. Линейные дифференциальные уравнения с переменными коэффициентами. Теорема существования и единственности решения для дифференциальных уравнений высших порядков. Линейный оператор и его свойства. Свойства решений линейного однородного дифференциального уравнения.

Тема 21. Экстремальные задачи теории графов: минимальное остовное дерево, кратчайший путь между вершинами, задача коммивояжера. Точные и приближенные алгоритмы для их решения: алгоритм Дейкстры, «жадные» алгоритмы

Задача коммивояжера, «жадный алгоритм». Задача о минимальном остовном дереве, алгоритмы Прима (растущее дерево) и Краскала (растущий лес). Задача о кратчайшем пути, алгоритм Дейкстры. Транзитивное замыкание. Алгоритм Флойда.

Тема 22. Комбинаторные операции: сочетания и размещения (с возвращением и без возвращения элементов). Комбинаторные принципы: сложение, умножение, дополнение, включение-исключение. Бином Ньютона. Полиномиальная формула

Основные комбинаторные принципы: принцип сложения, принцип умножения, принцип дополнения. Повторные выборки. Основные комбинаторные операции: выборки с возвращением и без возвращения элементов, с упорядочением и без упорядочения элементов, сочетания и размещения, числа сочетаний и размещений. Перестановки, разбиения. Принцип включения-исключения, диаграммы Эйлера.

Бином Ньютона, биномиальные коэффициенты, их основные свойства. Треугольник Паскаля. Полиномиальная формула, полиномиальные коэффициенты, их свойства.

Тема 23. Алфавитное кодирование: необходимое и достаточные условия однозначности декодирования. Теорема и алгоритм Маркова. Коды Хаффмана и Хэмминга

Слова и языки, операции над ними: сложение, умножение, итерация, дополнение. Регулярные выражения и регулярные языки, теорема Клини.

Задача анализа автомата-распознавателя, алгоритм для решения задачи анализа, представление распознаваемого языка в виде регулярного выражения.

Задача синтеза автомата-распознавателя по заданному регулярному выражению, недетерминированные двухполюсные источники, замкнутые множества состояний источника, преобразование источника в автомат.

Эквивалентные автоматы, эквивалентные состояния автомата, задача минимизации автоматов-распознавателей и автоматов-преобразователей, алгоритм Мили для решения задачи минимизации.

Раздел 2. Программирование

Тема 1. Работа с числами, превышающими возможности стандартных типов данных.

Алгоритмы «длинной» арифметики

Работа с числами в различных системах счисления в строковом формате. Алгоритмы «длинной» арифметики для вычислений с числами, выходящими за диапазоны стандартных типов данных.

Тема 2. Понятие структурного программирования. Принципы структурного программирования. Метод пошаговой детализации. Восходящее и нисходящее проектирование алгоритма

Понятие структурного программирования. Основные принципы структурного программирования. Основные положения метода пошаговой детализации. Пример применения метода пошаговой детализации к разработке программного обеспечения. Виды метода пошаговой детализации: восходящий и нисходящий, их отличительные особенности. Влияние указанных особенностей на процесс разработки программного обеспечения.

Тема 3. Сложность алгоритма. Оценка сложности нерекурсивных и рекурсивных алгоритмов. Понятие сложности задач. Классы сложности задач

Понятие сложности алгоритма. Параметры оценивания сложности алгоритма. Построение оценки сложности алгоритма для нерекурсивных и рекурсивных алгоритмов, примеры построения оценки сложности. Понятие сложности задач. Классы сложности задач P , EXP , NP , их особенности. Примеры задач, относящихся к соответствующим классам сложности.

Тема 4. Алгоритмическая машина Поста. Машина Тьюринга. Нормальный алгоритм Маркова

Понятие алгоритмических машин Поста и Тьюринга. Правила записи алгоритма с использованием машин Поста и Тьюринга. Понятие алгоритма Маркова. Правила записи алгоритма с использованием алгоритма Маркова. Примеры записи алгоритмов с использованием вышеуказанных средств.

Тема 5. Понятие информационного процесса. Виды информационных процессов.

Понятие информационных ресурсов, информационных систем. Эволюция информационных технологий. Классификация информационных систем

Информационный процесс. Передача, хранение, обработка информации. Канал передачи информации. Виды каналов.

Понятие информационных технологий. Информационные ресурсы. Информационная среда предприятия.

Эволюция информационных технологий от 40-х гг до настоящего времени. Влияние информационных технологий на процесс обработки информации на предприятии.

Понятие информационных систем. Классификация информационных систем. Корпоративные информационные системы. Интегрированные системы управления предприятием.

Тема 6. Стандартные требования при производстве ЭВМ. Стандартные методики измерения производительности ЭВМ. Альтернативные методики измерения производительности ЭВМ

Стандартные требования при производстве ЭВМ. Стандартная методика оценки производительности ЭВМ. Альтернативные методики оценки производительности ЭВМ: MIPS, MFLOPS, LINPACK, SPEC, TPC. Достоинства и недостатки альтернативных методик производительности.

Тема 7. Понятие сортировки. Параметры оценки алгоритмов сортировки.

Классификация сортировок. Характеристики внутренних методов сортировки.

Дополнительные факторы, учитываемые при сортировке. Хеширование.

Рехеширование

Понятие сортировки. Ключевая и информационная части сортируемого элемента. Основные параметры сортировки: по времени выполнения, по объему памяти, по распределению элементов, по значению элементов. Дополнительные параметры для определения алгоритма сортировки: размер данных, характеристики ключевой части сортируемого элемента, объем информационной части сортируемого элемента, программные связи, характеристики ЭВМ для реализации сортировки.

Общая классификация сортировок: внутренние и внешние сортировки.

Классификация внутренних сортировок: вставками, выбором, обменом, подсчетом. Общие алгоритмы классов.

Понятие хеширования. Хэш-функция, требования к ее построению, особенности построения хэш-функций. Понятие коллизии. Рехеширование. Виды рехеширования: линейное, случайное, квадратичное, метод цепочек.

Тема 8. Понятие рекуррентных вычислений. Правила написания программ, содержащих рекуррентные вычисления

Рекуррентная формула, порядок рекуррентной формулы. Виды рекуррентных формул. Правила записи программ, содержащих рекуррентные вычисления. Примеры записи программ, содержащих рекуррентные вычисления.

Тема 9. Понятие рекурсии. Правила написания программ, содержащих рекурсивные вычисления

Понятие рекурсии. Виды рекурсии: прямая, косвенная. Рекурсивный стек, правила его формирования. Прямой и обратный ход рекурсии. Правила написания программ, содержащих рекурсивные вычисления. Примеры записи программ, содержащих рекурсивные вычисления.

Тема 10. Понятие алгоритмов с возвратами. Правила написания программ, содержащих алгоритмы с возвратами

Понятие алгоритмов с возвратами. Область применения алгоритмов с возвратами. Эвристика. Правила написания программ, содержащих алгоритмы с возвратами. Примеры записи программ, содержащих алгоритмы с возвратами.

Тема 11. Понятие типа данных. Концепция типа данных. Пример характеристики типа данных

Понятие концепции типа данных. Основные положения концепции. Следствия из концепции. Понятие иерархии типов данных, базового типа данных, составного типа данных, мощности типа данных, скалярного типа данных. Правила построения характеристики типа данных. Построение характеристики для типов данных: integer, real, boolean, char, string, перечисление, ограничение, множество, массив, запись, типизированный файл, нетипизированный файл, текстовый файл. Построение характеристики для одного из типов данных: целый, плавающий, указатель, массив, перечисление, структура, смесь, файл..

Тема 12. Понятие дерева. Способы изображения деревьев. Способы представления деревьев. Обход дерева. Основные характеристики сбалансированных деревьев: идеально-сбалансированное дерево, АВЛ-дерево, красно-черное дерево, дерево случайного поиска, В-дерево

Понятие дерева, корня дерева, листа дерева, степени вершины, вершины-родителя, вершины-потомка, длина пути к вершине, глубина дерева. Бинарное дерево. Сильно-ветвящееся дерево.

Способы изображения деревьев: в виде вложенных множеств, вложенных скобок, с отступами, с помощью графа.

Способы представления деревьев: стандартная, обратная и расширенная формы представления.

Алгоритмы обхода дерева: прямой, обратный, концевой. Реализация алгоритмов обхода дерева. Особенности работы алгоритмов.

Понятие идеально-сбалансированного дерева, АВЛ-дерева, красно-черного дерева, дерева случайного поиска, В-дерева. Отличия в базовых алгоритмах работы с указанными деревьями.

Тема 13. Понятие графа. Способы изображения графов. Способы представления графов. Обход графа. Алгоритм нахождения кратчайшего пути в графе. Алгоритм нахождения множества достижимых вершин в графе

Понятие графа. Смежные вершины/ребра, инцидентные вершины/ребра, ориентированный граф, помеченный граф, петля в графе, маршруте графе, замкнутый маршрут, открытый маршрут, цепь в графе, цикл в графе, вес дуги, расстояние между вершинами, степень вершины. Способы изображения графов: текстовый, графический. Способы представления графов: матрица смежности, матрица инцидентности, список инцидентности, список ребер. Алгоритмы нахождения кратчайшего пути в графе, множества достижимых вершин.

Тема 14. Жизненный цикл программного обеспечения. Программы с большой и с малой жизнью. Этапы разработки программ по ГОСТ ЕСПД, по Майерсу. Технология макетирования. Модель водопада. Экстремальное программирование

Понятие жизненного цикла программ. Виды жизненных циклов: классический, по Глассу. Понятие программного продукта, программного комплекса. Требования к их созданию. Программы с малой и большой жизнью: принципиальные отличия, примеры. Этапы создания программ по ГОСТ ЕСПД, по Майерсу. Технология макетирования. Модель водопада. Итерационная модель. Спиральная модель. Экстремальное программирование.

Тема 15. Принятие решений при разработке программ. Формальное обоснование принятых решений. Вариантные сектора, вариантная сеть

Применение методики решения задач с помощью ЭВМ для видов задач: простейшие, содержащие основные управляющие структуры, содержащие рекуррентные соотношения, содержащие подпрограммы, содержащие обработку массивов, содержащие обработку файлов, содержащие рекурсию, содержащие алгоритмы с возвратами.

Тема 16. Порядок сборки программы. Методы тестирования программ. Методы отладки программ

Порядок сборки программ. Понятие тестирования. Принципы тестирования. Методы тестирования: инспекция исходного текста, сквозной просмотр, проверка за столом, "черный ящик", "белый ящик", пошаговое тестирование. Критерии завершения тестирования. Понятие отладки. Принципы отладки. Метод грубой силы, метод индукции, метод дедукции, отладка методом тестирования.

Тема 17. Особенности императивного программирования. Особенности функционального программирования. Функциональный стиль программирования.

Области применения функционального программирования. Функциональное программирование на F#.

Понятия императивного и функционального программирования, их особенности. Строго функциональный язык. Сравнение процедурного и функционального программирования. Функциональное программирование на F#: базовые типы, функции, каррирование, рекурсия, вывод типов, обобщенные функции. Кorteжи, списки. Представление знаний из различных предметных областей с помощью списков и corteжей. Операции над списками. Прямой конвейерный оператор. Прямой оператор композиции. Рекурсивная обработка списков.

Тема 18. Особенности логического программирования. Области применения языка

Пролог. Основы языка Пролог. Факты, правила, цель. Сопоставимость фактов

Особенности логического программирования. Области применения языка Пролог. Основы языка Пролог (факты, правила, цель, способ вычисления выражений, особенности переменных). Схема логического вывода. Конъюнкция и дизъюнкция в правиле и цели. Отрицание в правиле и цели. Управление перебором. Отсечение.

Тема 19. Основные понятия объектно-ориентированного программирования.

Принципы объектно-ориентированного программирования: инкапсуляция, наследование, полиморфизм. Исключения. Событийно-управляемое программирование

Основные понятия объектно-ориентированного программирования. Принципы объектно-ориентированного программирования: инкапсуляция, наследование, полиморфизм. Конструкторы, деструкторы, перегрузка. Исключения. Создание многоуровневой иерархии. Абстрактные классы. Абстрактные методы. Статические методы Событийно-управляемое программирование. Использование различных элементов управления. .

Тема 20. Структура компилятора. Основные функции составных частей компилятора.

Формальные и неформальные правила описания синтаксиса языка программирования
Понятие компилятора, его назначение. Составные части компилятора, их функции. Однопроходные и многопроходный компиляторы. Понятие синтаксиса языка программирования. Описание синтаксиса языка программирования с использованием диаграмм Вирта и форм Бэкуса-Наура. Примеры. Неформальные правила описания синтаксиса языка программирования.

Тема 21. БД и СУБД. Основные функции СУБД. Многоуровневая архитектура современных СУБД

Основные требования к организации СУБД. Функции СУБД. Минимальная избыточность. Независимость данных. Управление данными, управление транзакциями. Журнализация. Восстановление после сбоев.

Многоуровневая архитектура современных СУБД. Понятие модели данных с точки зрения многоуровневой архитектуры СУБД (инфологическая, внешние, концептуальная, логическая и физическая модели данных). Логическая и физическая независимость данных. Физическая организация данных в БД. Методы хранения и доступа к данным (последовательный, индексно-последовательный, прямой, В-деревья).

Тема 22. Понятие модели данных (МД). Основные компоненты МД. Традиционные МД. Отличительные особенности семантических МД

Понятие модели данных. Основные компоненты модели данных: структуры, ограничения целостности, операции. Взаимосвязи в модели данных («один к одному», «один ко многим», «многие к одному», «многие ко многим»). Традиционные (синтаксические) и семантические модели данных. Отличительные особенности семантических МД.

Тема 23. Понятие распределенных БД. Хранилища данных. Свойства хранилищ данных. Технологии хранилищ данных

Понятие распределенных БД. Свойства распределенных БД. Принципы построения распределенных БД. Понятие хранилищ данных. Отличительные особенности хранилищ данных. Свойства хранилищ данных. Принципы организации хранилищ данных. Технологии хранилищ данных.

Тема 24. Жизненный цикл БД. Классификация и анализ рынка промышленных СУБД
Этапы жизненного цикла БД: планирование разработки БД, определение требований, проектирование БД, реализация, тестирование БД, эксплуатация и сопровождение БД. Классификация промышленных СУБД. Требования к промышленным СУБД. Сравнение промышленных СУБД.

Тема 25. Понятие модели информационной системы (ИС). Статическая, динамическая и функциональная модели ИС; связь между ними; относительная важность.

Концептуальная модель, модель спецификации и модель реализации; различия в интерпретации. Понятие метамодели

Понятие информационной системы (ИС). Выявление задач, стоящих перед разработчиком ИС. Определение критерия качества ИС. Выявление проблемы сложных задач (проблема разбиения, проблема языка, проблема процесса). Понятие методологии и технологии. Статическая, динамическая и функциональная модели ИС; связь между ними; относительная важность. Концептуальная модель, модель спецификации и модель реализации; различия в интерпретации. Понятие метамодели.

Тема 26. Язык UML, определение и назначение. Обзор основных диаграмм языка.

Возможности их применения на различных этапах жизненного цикла информационной системы

Определение сущности объектно-ориентированного подхода. Знакомство с основными концепциями унифицированного языка моделирования UML. Изучение моделирования функциональных требований, бизнес-процессов, концептуального моделирования и соответствующих диаграмм UML. Освоение проектирования поведения ИС, ее статической структуры и соответствующих диаграмм UML. Изучение моделирования реализации и развертывания системы и соответствующих диаграмм UML. Изучение шаблонов проектирования.

Раздел 3. Защита информации

Тема 1. Процессоры компании Intel. Архитектура процессоров IA-32.

Микроархитектура процессоров Intel

История развития компании Intel. Основные направления развития процессоров. Архитектура x86. Микроархитектура: тракт данных, регистры и т.д.

Тема 2. Процессоры Intel в реальном режиме: регистры процессора, управление памятью и программами, данные и способы адресации, система команд, система прерываний

Процессоры Intel в реальном режиме: регистры процессора, управление памятью и программами, данные и способы адресации, система команд, система прерываний.

Тема 3. Процессоры Intel в защищенном режиме: регистры процессора, управление памятью, поддержка многозадачности и защита памяти

Процессоры Intel в защищенном режиме: регистры процессора, управление памятью, поддержка многозадачности и защита памяти.

Тема 4. Архитектура ядра RISC микроконтроллера Atmel

Основные характеристики микроконтроллера Atmel. Архитектура ядра RISC микроконтроллера. Порты ввода-вывода. Прерывания микроконтроллера. Аналого-цифровой преобразователь в составе микроконтроллера.

Тема 5. Основы программирования микропроцессорных систем

Система команд микропроцессора: команды передачи данных между регистрами, команды арифметических операций, команды логических операций, команды передачи управления или перехода, специальные команды. Общие правила записи команд.

Тема 6. Информационная безопасность в системе национальной безопасности

Российской Федерации. Система обеспечения информационной безопасности России

Основные элементы системы безопасности Российской Федерации на основании положений Российского законодательства. Элементы системы информационной безопасности как подсистемы национальной безопасности. Основные правовые нормы деятельности субъектов системы информационной безопасности и их взаимосвязь.

Тема 7. Основные понятия информационной безопасности. (ФЗ «О безопасности», «Об информации, информационных технологиях и о защите информации», Стратегия национальной безопасности РФ, Доктрина информационной безопасности РФ, ГОСТ Р 50922-2006; системный подход). Общеметодологические принципы теории ИБ (общие понятия информационной безопасности, их взаимосвязь по ГОСТ Р ИСО/МЭК 15408, “Общие критерии”)).

Терминология категории «безопасность» в соответствии с Российским законодательством. Понятия: безопасность, жизненно важные интересы, основные объекты безопасности, опасность, ущерб, угроза безопасности, вызов, обеспечение безопасности. Схема деятельности по обеспечению безопасности, основные принципы обеспечения безопасности, классификация видов безопасности. Классификация правовой основы системы информационной безопасности Российской Федерации. Основные правовые нормативные документы, регламентирующие деятельность в сфере информационной безопасности России: ФЗ «О безопасности», Доктрина информационной безопасности, Стратегия национальной безопасности, ГОСТ Р 50922-2006.

База организационно-технических документов, регламентирующих основные базовые понятия, их взаимосвязь, взаимодействие. Базовые основы по ЗИ в организационно-технических документах: ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности. Критерии оценки; ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью; и др..

Тема 8. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Понятия “менеджмента информационной безопасности”, “Политики информационной безопасности”

Нормативный документ ГОСТ Р ИСО/МЭК 27002-2012 Менеджмент информационной безопасности. Политика информационной безопасности. Описание, основные положения, область действия.

Тема 9. Четырехуровневая система как метод анализа информационной безопасности

Четырехуровневая система как метод анализа информационной безопасности. Законодательный уровень. Административный уровень. Процедурный уровень. Программно-технический уровень.

Тема 10. Уголовно – правовая характеристика состава преступлений, предусмотренных ст.272-274 Уголовного кодекса РФ

Понятия: состав преступления, объект преступления, субъект преступления, объективная сторона преступления, субъективная сторона преступления. Статьи 272-274 Уголовного кодекса РФ: содержание, область действия, виды наказаний.

Тема 11. Организация государственного контроля и надзора за соблюдением требований к защите информации в РФ

Основные государственные органы, отвечающие за контроль и надзор за соблюдением требований к защите информации в РФ: Совет безопасности РФ, ФСБ России, ФСТЭК России, ФСО России, Роскомнадзор. Их основные функции.

Тема 12. Классификация информации с точки зрения ФЗ «Об информации, информационных технологиях и о защите информации»

Понятие информации с точки зрения ФЗ «Об информации, информационных технологиях и о защите информации». Классификация информации в зависимости ее предоставления и распространения. Классификация информации в зависимости от категории доступа к ней. Информация, доступ к которой не может быть ограничен. Информация ограниченного доступа.

Тема 13. Информация как предмет частных правоотношений

Понятие информационного права. Частное и публичное право, их понятие и соотношение. Критерии разграничения публичного и частного права. Критерии отнесения норм к частному праву.

Тема 14. Информация как предмет публичных правоотношений

Понятие информационного права. Частное и публичное право, их понятие и соотношение. Критерии разграничения публичного и частного права. Критерии отнесения норм к публичному праву.

Тема 15. Стандарт ISO 27000

Серия стандартов ISO/IEC 27000: основное назначение, область применения. Основные термины и определения: актив, информационный актив, информационная безопасность, система менеджмента информационной безопасности, риски информационной безопасности. Процессный подход для систем менеджмента информационной безопасности.

Тема 16. Стандарт BSI (Германия). Федеральные критерии безопасности информационных технологий (США). Международный стандарт COBIT

Назначение стандарта BSI. Основные разделы стандарта BSI. Виды угроз в стандарте BSI. Классификация контрмер в стандарте BSI. Назначение и цели разработки стандарта «Федеральные критерии безопасности информационных технологий». Основные положения стандарта «Федеральные критерии безопасности информационных технологий». Основное назначение международного стандарта COBIT. Состав международного стандарта COBIT. Основные положения международного стандарта COBIT.

Тема 17. Общие требования по защите информации, предусмотренные РД, Приказом №17, Требованиями и Положениями ФСТЭК России, СТР-К

Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Специальные требования и рекомендации по технической защите конфиденциальной информации. Приказ ФСТЭК №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Описание, основные термины и определения, основные положения, область действия.

Тема 18. Общие нормативные требования по защите персональных данных
Федеральный закон №152-ФЗ «О персональных данных». Постановление правительства №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Приказ ФСТЭК №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Описание, область действия, основные понятия, основные положения.

Тема 19. Алгоритмы блочного шифрования. ГОСТ Р 34.12-2015
Понятие блочного шифра. ГОСТ Р 34.12-2015 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры». Область применения, основные термины и определения. Алгоритм блочного шифрования с длиной блока 64 бит. Алгоритм блочного шифрования с длиной блока 128 бит.

Тема 20. Алгоритмы шифрования с открытым ключом. Алгоритм RSA.
Понятие алгоритма шифрования с открытым ключом. Отличия алгоритмов шифрования с открытым ключом от алгоритмов шифрования с закрытым ключом. Применение алгоритмов шифрования с открытым ключом. Алгоритм RSA. Генерация ключей RSA. Алгоритмы шифрования и дешифрования.

Тема 21. Криптографические хеш-функции. ГОСТ Р 34.11-2012
Понятие хеш-функции. Применение хеш-функций. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хеширования». Область применения, основные термины и определения. Процедура вычисления хеш-функции.

Тема 22. Электронная подпись. ГОСТ Р 34.10-2012
Понятие электронной подписи. Простая электронная подпись, усиленная неквалифицированная электронная подпись, усиленная квалифицированная электронная подпись. Использование электронной подписи. ГОСТ 34.10-2012 «Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Область применения, основные термины и определения. Генерация ключей. Формирование подписи. Проверка подписи.

Тема 23. Режимы блочного шифрования ГОСТ Р 34.13-2015
Режимы работы блочных шифров. ГОСТ Р 34.13-2015 «Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров». Область применения, основные термины и определения. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью по выходу. Режим простой замены с зацеплением. Режим гаммирования с обратной связью по шифротексту. Режим выработки имитовставки.

Тема 24. Криптографический генератор псевдослучайных чисел
Генератор псевдослучайных чисел. Критерии, которым должен удовлетворять генератор псевдослучайных чисел. Криптографически стойкий генератор псевдослучайных чисел. Требования к криптографически стойкому генератору псевдослучайных чисел. Классы реализации криптографически стойкого генератора псевдослучайных чисел: на основе криптографических алгоритмов, на основе вычислительно сложных математических задач, специальные реализации.

Тема 25. Протокол SSL
Назначение протокола SSL. Принцип работы протокола SSL: фаза рукопожатия и фаза передачи данных. Используемые протоколы: протокол рукопожатия, протокол изменения параметров шифра, протокол тревоги. Процедура рукопожатия между клиентом и сервером. SSL-сертификаты, способы их получения.

Тема 26. Протокол Kerberos
Назначение протокола Kerberos. Принцип работы протокола Kerberos. Управление ключами, центр распределения ключей KDC. Сервер аутентификации и сервер выдачи мандатов и разрешений.

Тема 27. Протоколы аутентификации
Понятия идентификации, аутентификации и авторизации. Аутентификация по паролю. Аутентификация по сертификатам. Принцип работы протоколов HTTP, HTTPS, SSL/TLS, Kerberos.

Тема 28. Сравнительная характеристика моделей OSI и TCP/IP

Уровни модели OSI и TCP/IP. Примеры протоколов работающих на разных уровнях. Связи между уровнями. MTU и фрагментация на разных уровнях. Примеры нарушения связи уровней.

Тема 29. Протоколы модемной связи

Понятие модема. Протоколы модемной связи физического уровня. Международные протоколы модемной связи физического уровня. Фирменные протоколы модемной связи физического уровня. Протоколы модемной связи канального уровня. Виды протоколов модемной связи канального уровня: старт-стоп протоколы, конвейерные протоколы. Протокол XModem, XModem-CRC, YModem, ZModem.

Тема 30. Протоколы маршрутизации

Процесс и принципы маршрутизации по назначению. Рекурсивный просмотр таблицы маршрутизации. Метрика, административная дистанция, область видимости маршрута. Процесс построения таблицы маршрутизации. Маршрутизация по политике. Статическая маршрутизация. Маршрутизация по-умолчанию. Плавающие маршруты. Маршрутизация по политике. Динамическая маршрутизация. Основные принципы. Механизмы блокировки циклов. Редистрибьюция маршрутов. Протоколы OSPF, EIGRP, BGP. Автономная система. Архитектура Интернет. Иерархия операторов связи. Автономные системы. Провайдеронезависимые блоки адресов. БД маршрутной информации. Услуга «IP-транзит». Отношения «пиринга». Точки обмена трафиком. Правила BGP-multihoming. Фильтрация маршрутной информации. Работа с BGP full-feed.

Тема 31. Протоколы туннельной передачи данных

Понятие туннелирования. Назначение протоколов туннельной передачи данных. Принцип действия протоколов PPTP и L2TP.

Тема 32 Реализация системы защиты операционных систем семейства Microsoft Windows

Методы, средства и возможности реализации системы защиты операционных систем Microsoft Windows.

Тема 33. Реализация системы защиты UNIX-подобных операционных систем

Методы, средства и возможности реализации системы защиты операционных систем Unix/Linux.

Тема 34. Управление процессами и потоками: представление процессов и потоков в операционных системах, дисциплины планирования процессов, взаимодействие процессов, проблема тупиков

Постановка задачи управления процессами и ресурсами как фундаментальная задача современных операционных систем. Принципы решения этих задач в современных операционных системах, приводятся примеры.

Проблема взаимного исключения параллельно работающих процессов при обработке разделяемых ресурсов. Основные способы решения этой проблемы в привязке к механизмам и средствам, реализованным для этого в современных операционных системах.

Проблема тупика, как проблема, вытекающая из организации некорректного взаимного исключения. Теоретические основы детектирования и устранения тупиков. Средства защиты от тупиков и разрешения тупиков, реализованные в современных операционных системах.

Основные механизмы планирования и диспетчеризации процессов в современных операционных системах. Примеры планирования и диспетчеризации. Переключение процессора с задачи на задачу.

Тема 35. Управление оперативной памятью: управление физической и виртуальной памятью, реализация свопинга

Описываются механизмы управления памятью, реализованные в современных операционных системах. Рассматривается стековая организация памяти, организация кучи, сегментно-страничная организация памяти, схема трансляции адреса и механизм виртуализации памяти (подкачка).

Тема 36. Управление файловыми системами: организация дискового пространства, современные файловые системы

Файловые системы: виды, типы, отличия, сравнение. Организация дискового пространства на уровне файловой системы на примере. Основные современные файловые системы и их особенности.

Тема 37. Вредоносные программы: классификация, основные характеристики, современные тенденции в развитии вредоносных программ

Понятие вредоносного программного обеспечения. Основные характеристики вредоносного программного обеспечения: целевая среда, объекты-носители, механизмы запуска, механизмы распространения, механизмы защиты, вредоносное действие. Классификация вредоносного программного обеспечения: вирусы, черви, троянские программы, бот-сети, эксплойты. Примеры вредоносного программного обеспечения. Современные тенденции в развитии вредоносных программ: стелс-вирусы, полиморфные вирусы.

Тема 38. Компьютерные вирусы: классификация, основные характеристики, способы внедрения в программный код, способы сокрытия факта заражения и основные демаскирующие признаки

Понятие компьютерного вируса. Отличительные особенности компьютерных вирусов от другого вредоносного программного обеспечения. Классификация компьютерных вирусов по объекту-носителю: вирусы для исполняемых файлов (СОМ-вирусы, ЕХЕ-вирусы), загрузочные вирусы (ВООТ-вирусы), макровирусы, скрипт-вирусы. Классификация компьютерных вирусов по способу заражения: классические (внедряемые) вирусы, вирусы-вандалы, вирусы-спутники. Способы внедрения компьютерного вируса в программный код: внедрение вируса в начало файла, в середину файла, в конец файла. Способы сокрытия факта заражения: маскировка, шифрование. Основные демаскирующие признаки компьютерных вирусов: сигнатура вируса, эвристические признаки.

Тема 39. Антивирусные программы: классификация антивирусных программ, способы обнаружения и уничтожения вредоносного кода, характеристика современных антивирусных программ

Понятие антивирусного программного обеспечения. Основные задачи и функции антивирусного программного обеспечения. Требования к современному антивирусному программному обеспечению. Классификация антивирусного программного обеспечения: программы-детекторы, программы-мониторы, программы-доктора, программы-ревизоры, программы-фильтры, комплексные антивирусы. Методы обнаружения вредоносного программного обеспечения: сигнатурный анализ, эвристический анализ, метод контроля целостности, метод отслеживания поведения программ.

Тема 40. Угрозы информационной безопасности программного обеспечения. Модели безопасности информационных систем

Виды угроз информационной безопасности программного обеспечения. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» Область применения. Понятия объекта оценки, профиля защиты, задания по безопасности. Взаимосвязь между содержанием профиля защиты, задания по безопасности и объекта оценки. Основные понятия безопасности и их взаимосвязь. Основные понятия, используемые при оценке, и их взаимосвязь.

Тема 41. Функциональные требования безопасности: методика формирования требований, реализация функциональных требований безопасности

ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности». Область применения. Парадигма функциональных требований. Классы функциональных требований, их характеристика.

Тема 42. Требования доверия к безопасности информационных систем: методика формирования требований, поддержание доверия к безопасности информационных систем и программных продуктов

ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

Часть 3. Компоненты доверия к безопасности». Область применения. Шкала оценки доверия в ИСО/МЭК 15408. Классы требований доверия к безопасности, их характеристика.

Тема 43. Классификация технических каналов утечки информации

Виды технических каналов утечки информации, их краткая характеристика. Существующие подвиды технических каналов, их краткая характеристика.

Тема 44. Виды и источники носителей защищаемой информации

Классификация информации, защищаемой техническими средствами. Видовые демаскирующие признаки, их классификация. Сигнальные демаскирующие признаки. Демаскирующие признаки веществ. Классификация опасных сигналов. .

Тема 45. Виды контроля эффективности защиты информации

Классификации видов контроля эффективности защиты информации. Основные характеристики предварительного, периодического и постоянного контроля. Основные виды технического контроля: инструментальный контроль, инструментально-расчетный контроль, расчетный контроль. Организационные меры контроля эффективности защиты информации.

Тема 46. Оценка угроз акустических каналов утечки информации. Непреднамеренное прослушивание. Технические средства контроля звукоизоляции ограждающих конструкций

Основные технические каналы утечки акустической информации, оценка опасности указанных каналов. Отличие непреднамеренного прослушивания от разведки. Перечень технических средств контроля звукоизоляции ограждающих конструкций и их краткая характеристика.

Тема 47. Порядок и методика аттестации защищаемых помещений

Методы проведения аттестации защищаемых помещений, их характеристика. Программа проведения аттестационных испытаний. Понятие методики аттестации. Критерий выбора вида методики аттестации в зависимости от вида защищаемого помещения.

Тема 48. Порядок выявления специальных электронных устройств негласного перехвата информации в средствах вычислительной техники при подготовке к аттестации по требованиям безопасности информации

Методы выявления физического наличия закладного устройства в изделии. Методы выявления Недекларируемых возможностей в программном обеспечении. Методы выявления беспроводных соединений в исследуемом средстве.

Тема 49. Контроль целостности аппаратных, программных ресурсов и гарантированное уничтожение информации

Понятие контроля целостности аппаратных и программных ресурсов. Примеры программных комплексов, имеющих функцию контроля целостности аппаратных и программных ресурсов. Методы контроля целостности аппаратных и программных ресурсов: статический и динамический, их характеристика. Гарантированное уничтожение информации. Примеры программных комплексов, имеющих функцию гарантированного уничтожения информации. Механизм затирания в Secret Net.

Тема 50. Управление доступом. Дискреционный и мандатный методы доступа.

Изолированная программная среда

Понятия дискреционного и мандатного разграничения доступа. Описание механизма «Разграничение доступа» в Secret Net. Режимы работы механизма «Разграничение доступа» в Secret Net: контроль потоков, контроль печати, регистрация событий. Механизм замкнутой программной среды. Режимы работы механизма замкнутой программной среды.

Тема 51. Автоматизированные средства защиты информации от НСД

Автоматизированные средства защиты информации от НСД: Ревизор, Страж NT, Аккорд, Secret Net, Dallas Lock. Их назначение, функционал, возможности.

Тема 52. Архитектурные особенности и транзакционные модели современных СУБД

Основные компоненты СУБД: БД, сервер, клиент. Связь между ними. Понятие транзакции. Проблемы, возникающие при работе множества пользователей: потеря изменений, грязное чтение, невозпроизводимое чтение, фантомные строки, перекрывающиеся транзакции. Основные состояния транзакций. Основные показатели транзакций. Контекст транзакции.

Тема 53. Разграничение доступа в современных СУБД

Понятия объект доступа, субъект доступа, правила разграничения доступа. Пользователи СУБД: администраторы базы данных и конечные пользователи базы данных. Привилегии, назначение привилегий. Понятие роли. Основные требования и условия применения ролей.

Тема 54. Защита информации на уровне сервера

Система безопасности уровня сервера. Аутентификация пользователей на уровне сервера. Встроенные роли сервера.

Тема 55. Защита информации на уровне базы данных

Система безопасности уровня базы данных. Пользователи базы данных. Привилегии, назначение привилегий. Понятие роли. Встроенные роли базы данных.

Тема 56. Администрирование современных СУБД. Обеспечения безопасности данных в современных СУБД на примере СУБД Oracle. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных

Администрирование современных СУБД. Обеспечения безопасности данных в современных СУБД на примере СУБД Oracle. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных.

Тема 57. Администрирование современных СУБД. Обеспечения безопасности данных в современных СУБД на примере СУБД Firebird. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных

Администрирование современных СУБД. Обеспечения безопасности данных в современных СУБД на примере СУБД Firebird. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных.

Тема 58. Защита инфраструктуры маршрутизации

Методы и средства защиты инфраструктуры маршрутизации отказоустойчивых компьютерных сетей. Настройка протокола OSPF, который обеспечивает корректную работу сети и защиту инфраструктуры маршрутизации.

Тема 59. Защита инфраструктуры коммутации

Методы и средства защиты инфраструктуры коммутации при использовании технологии виртуальных ЛВС. Статические и динамические виртуальные ЛВС.

Тема 60. Защита сетевой инфраструктуры

Методы и средства защиты сетевой инфраструктуры от НСД, принципы проектирования сетей управления.

Тема 61. Защита периметра сети

Основные технологии межсетевого экранирования, методы и средства управления безопасностью информационных потоков на межсетевых экранах и сетевых маршрутизаторах.

Тема 62. Криптографическая защита каналов передачи данных

Методы и средства защиты каналов передачи данных ГВС на основе технологии виртуальных частных сетей. Семейство протоколов IPSec.

Тема 63. Роль эффективных коммуникаций в информационной безопасности предприятия

Понятие эффективного коммуникативного процесса. Средства коммуникации, примеры. Барьеры коммуникации: шумы и фильтры. Психологические фильтры, физиологические фильтры, лингвистические фильтры, логические фильтры, социокультурные фильтры. Вертикальные и горизонтальные коммуникации. Характеристики безопасных организационных коммуникаций.

Тема 64. Мотивация работника в структуре политики безопасности предприятия

Понятие мотивации. Внешняя и внутренняя мотивация. Первичные и вторичные мотивы. Потребности сотрудников, влияющие на удовлетворенность трудом. Методы стимулирования труда: позитивное подкрепление, негативное подкрепление, вознаграждение, экономический метод, целевой метод, адаптивно-организационный метод. Дифференцированный подход к стимулированию персонала. Типичные ошибки в реализации функции стимулирования.

Тема 65. Психологические методы ведения информационно-психологической войны

Понятие информационно-психологической войны. Способы ведения информационно-психологической войны: дробление информации, немедленность передачи информации, перехват инициативы. Воздействие через социальные институты. Общественное мнение. Способы воздействия на общественное мнение: СМИ, продуцирование необходимых слухов, проведение опросов общественного мнения.

Тема 66. Роль организационной культуры в создании эффективной системы безопасности предприятия

Понятие организационной культуры. Уровни организационной культуры: символический, подповерхностный и глубинный уровни. Компоненты организационной культуры. Доминирующая культура и субкультура. Виды субкультур: «передовая» субкультура, «неконфликтующая» субкультура, контркультура, «теневая» субкультура. Типы работников по отношению к ценностям и нормам организации, их характеристика.

Тема 67. Способы и приемы безопасной кадровой политики на предприятии

Понятие кадровой политики. Цели кадровой политики в соответствии со стадиями жизненного цикла организации. Этапы процедуры отбора кандидатов на вакансию. Безопасные способы увольнения сотрудника. Общие мероприятия безопасного увольнения сотрудника.

Тема 68. Роль групповой динамики в поддержании информационной безопасности предприятия

Понятие динамики группы. Групповые роли. Классификация групповых ролей по психологической позиции в группе. Функции групповых ролей. Групповые процессы и групповые состояния. Групповые эффекты. Уровни развития группы.

Тема 69. Алгоритм RSA. Принцип работы, взаимная обратность отображений шифрования и дешифрования, вопросы выбора параметров, приложения, основные виды атак

Алгоритм RSA. Генерация ключей RSA. Алгоритмы шифрования и дешифрования. Взаимная обратность отображений шифрования и дешифрования. Выбор параметров. Основные виды атак: атаки на основе алгоритмов разложения на множители, атаки на основе алгоритмов вычисления дискретного логарифма, атака Винера, атака на подпись RSA в схеме с нотариусом.

Тема 70. Методы факторизации натуральных чисел

Понятие факторизации натуральных чисел. Методы факторизации натуральных чисел: экспоненциальные алгоритмы и субэкспоненциальные алгоритмы. Примеры факторизации натуральных чисел. Перебор делителей. Алгоритм факторизации Ферма. Метод Полларда.

Тема 71. Эллиптические кривые в криптографии

Эллиптические кривые. Групповой закон для эллиптических кривых. Геометрическое сложение и алгебраическое сложение. Эллиптические кривые над конечными полями. Скалярное умножение и циклические подгруппы. Криптография на эллиптических кривых. Шифрование с помощью ECDH. Алгоритм ECDSA.

4.2. Критерии оценки результатов сдачи государственного экзамена

4.2.1. Показатели и критерии оценивания компетенций

4.2.1.1. Показатели и критерии оценивания ОК-компетенций

| Код компетенции | Наименование компетенции | Показатели оценивания | Критерии оценивания | Способ / Средство оценивания |
|-----------------|---|--|--|--|
| ОК-2 | владеть навыками коммуникации, уметь аргументировано и грамотно строить устную и письменную речь на русском языке, способность к общению в социальной и производственной деятельности | владение навыками коммуникации, умение аргументировано и грамотно строить устную и письменную речь на русском языке, способностью к общению в социальной и производственной деятельности | Знать: основы социальной и производственной деятельности. Уметь: аргументировано и грамотно строить устную и письменную речь на русском языке. Владеть: навыками коммуникации. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ОК-6 | способность анализировать социально значимые проблемы и процессы | способностью анализировать социально значимые проблемы и процессы | Знать: социально значимые проблемы и процессы. Уметь: анализировать социально значимые проблемы и процессы. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ОК-7 | знать и уважать историческое наследие и культурные традиции своей страны, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия, способность анализировать основные этапы и закономерности исторического развития общества | знание и уважение исторического наследия и культурных традиций своей страны, толерантное восприятие социальных, этнических, конфессиональных и культурных различий, способностью анализировать основные этапы и закономерности исторического развития общества | Знать: историческое наследие и культурные традиции своей страны. Уметь: анализировать основные этапы и закономерности исторического развития общества. Владеть: навыками толерантного восприятия социальных, этнических, конфессиональных и культурных различий. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ОК-9 | владеть базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях, способность приобретать новые знания, используя современные информационные технологии | владение базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях, способностью приобретать новые знания, используя современные информационные технологии | Знать: основы информатики. Уметь: приобретать новые знания, используя современные информационные технологии. Владеть: базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |

| | | | | |
|-------|---|---|--|--|
| ОК-10 | понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны | понимание сущности и значения информации в развитии современного общества, соблюдение основных требований информационной безопасности, в том числе защиты государственной тайны | Знать: сущность и значение информации в развитии современного общества. Уметь: соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
|-------|---|---|--|--|

4.2.1.2. Показатели и критерии оценивания ОПК-компетенций

| Код компетенции | Наименование компетенции | Показатели оценивания | Критерии оценивания | Способ / Средство оценивания |
|-----------------|--|---|---|--|
| ОПК-1 | способность использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с математическими и компьютерными науками | способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с математическими и компьютерными науками | Знать: основные факты, концепции, принципы теорий, связанных с математическими и компьютерными науками. Уметь: использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с математическими и компьютерными науками, в сфере своей деятельности. Владеть: навыками использования базовых знаний естественных наук, математики и информатики, основных фактов, концепций, принципов теорий, связанных с математическими и компьютерными науками. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ОПК-3 | способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением | способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической | Знать: основные требования информационной безопасности. Уметь: решать стандартные задачи профессиональной деятельности на | Ответы на вопросы экзаменационного билета, членов государственной комиссии |

| | | | | |
|-------|---|--|---|--|
| | информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. | |
| ОПК-5 | способность действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма | готовностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма | Знать: основные положения Конституции Российской Федерации. Уметь: действовать в соответствии с Конституцией Российской Федерации, исполняя свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ОПК-6 | способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства | способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства | Знать: социальную значимость своей будущей профессии, цели и смысл государственной службы. Владеть: высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |

4.2.1.3. Показатели и критерии оценивания ПК-компетенций

| Код компетенции | Наименование компетенции | Показатели оценивания | Критерии оценивания | Способ / Средство оценивания |
|-----------------|---|--|---|--|
| ПК-1 | способность взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий | способностью взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий | Знать: профессиональные сетевые сообщества, способы взаимодействия и сотрудничества с профессиональными сетевыми сообществами. Уметь: отслеживать динамику развития выбранных направлений области информационных технологий. Владеть: навыками взаимодействия и сотрудничества с профессиональными сетевыми сообществами. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ПК-3 | способность к анализу и формализации поставленных задач в области информационной безопасности | способностью к анализу и формализации поставленных задач в области информационной безопасности | Знать: основные задачи в области информационной безопасности. Уметь: формализовать поставленные задачи в области информационной безопасности. Владеть: методами анализа поставленных задач в области информационной безопасности. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ПК-4 | способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности | способностью проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов области компьютерной безопасности | Знать: отечественные и зарубежные стандарты в области компьютерной безопасности. Уметь: проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов области компьютерной безопасности. Владеть: основными методами проведения анализа безопасности компьютерных систем с использованием отечественных и зарубежных стандартов области компьютерной безопасности. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |

| | | | | |
|------|---|--|--|--|
| ПК-6 | способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем | способностью разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем | Знать: правила разработки математических моделей защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. Уметь: разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. Владеть: математическим аппаратом для разработки математических моделей защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ПК-7 | способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований | способностью провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований | Знать: правила обоснования и выбора рациональных решений; уровни обеспечения информационной безопасности. Уметь: выбирать рациональные решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований. Владеть: навыками обоснования и выбора рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |

| | | | | |
|-------|--|--|---|--|
| ПК-11 | способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи | способностью оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи | Знать: правила оценки степени надежности механизмов обеспечения безопасности. Уметь: оценивать степень надежности механизмов обеспечения безопасности. Владеть: методами оценивания степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ПК-12 | способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований | готовностью участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований | Знать: правила проведения экспериментально-исследовательских работ при аттестации системы защиты информации; требования к системам защиты информации. Уметь: участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований. Владеть: навыками аттестации системы защиты информации с учетом требований. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ПК-22 | способность использовать нормативные правовые документы в своей профессиональной деятельности | способностью использовать нормативные правовые документы в своей профессиональной деятельности | Знать: существующие нормативные правовые документы в своей профессиональной деятельности. Уметь: использовать нормативные правовые документы в своей профессиональной деятельности. Владеть: навыками использования нормативных правовых документов в своей профессиональной деятельности. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |

| | | | | |
|-------|--|---|--|--|
| ПК-23 | способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами | способностью организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами | Знать: технические и программные средства защиты данных. Уметь: организовать защиту информации техническими и программными средствами. Владеть: приемами антивирусной защиты при работе с компьютерными системами. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
|-------|--|---|--|--|

4.2.1.4. Показатели и критерии оценивания ПСК-компетенций

| Код компетенции | Наименование компетенции | Показатели оценивания | Критерии оценивания | Способ / Средство оценивания |
|-----------------|---|--|---|--|
| ПСК-3 | способность руководствоваться требованиями современных стандартов по безопасности компьютерных систем | готовностью руководствоваться требованиями современных стандартов по безопасности компьютерных систем | Знать: российские и международные стандарты по компьютерной безопасности. Уметь: грамотно руководствоваться требованиями современных стандартов по безопасности компьютерных систем. Владеть: навыками применения стандартов безопасности к проектированию и разработке компьютерных систем в соответствии с требованиями к безопасности компьютерных систем. | Ответы на вопросы экзаменационного билета, членов государственной комиссии |
| ПСК-6 | способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности | способностью применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности | Знать: классификацию и назначение языков и систем программирования, средств прикладного, системного и специального назначения. Уметь: применять современные инструментальные средства программирования для разработки программного обеспечения различного назначения; применять средства прикладного, системного и специального назначения в | Ответы на вопросы экзаменационного билета, членов государственной комиссии |

| | | | | |
|--|--|--|---|--|
| | | | профессиональной деятельности. Владеть: навыками применения языков, систем и инструментальных средств программирования, навыками работы с программными средствами прикладного, системного и специального назначения в профессиональной деятельности. | |
|--|--|--|---|--|

4.2.2. Шкала и критерии оценки государственного экзамена

| Шкала оценивания | Критерии оценки |
|---------------------|---|
| неудовлетворительно | <p>Ответ не соответствует заявленному экзаменационному вопросу, его содержание не раскрыто, теоретические знания отсутствуют.</p> <p>Студент не демонстрирует наличие сформированных компетенций</p> <ul style="list-style-type: none"> • Не демонстрирует умение показать сформированность компетенций вопроса государственного экзамена в ответе. • Не демонстрирует знания в области вопросов билета государственного экзамена. • Не демонстрирует опыт использования полученных знаний из теоретической работы и практической. |
| удовлетворительно | <p>Не в полном объеме ответил на заданные вопросы. Обнаружил неполные знания теоретических основ, допускал существенные неточности в изложении, не всегда корректно употреблял терминологию. Ответ слабо структурирован, не аргументирован, практически не иллюстрирован ссылками на исследования, не содержит собственных наблюдений и примеров.</p> <p>Соответствует критериям в рамках одного билета в частичном объеме:</p> <ul style="list-style-type: none"> • Демонстрирует фрагментарный опыт использования теоретических и практических знаний. • Демонстрирует частично сформированное умение показать сформированность компетенций вопроса государственного экзамена в ответе. • Демонстрирует частично сформированное знание в области вопросов билета государственного экзамена. |
| хорошо | <p>Ответил на заданные вопросы, но при этом имела место неполнота ответа и неточности, которые потребовали дополнительных вопросов и уточнений. Ответ структурирован и в основном аргументирован, в целом последовательно изложен, но слабо иллюстрирован ссылками на исследования и примерами из практики, не содержит собственных выводов.</p> <p>Соответствует критериям в рамках одного билета не в полном объеме:</p> <ul style="list-style-type: none"> • Демонстрирует в целом успешный, но содержащий отдельные пробелы опыт использования теоретических и практических знаний. • Демонстрирует сформированное, но содержащее отдельные пробелы умение показать сформированность компетенций вопроса государственного экзамена в ответе. • Демонстрирует сформированное, но содержащее отдельные пробелы знание в области вопросов билета государственного экзамена. |

| | |
|---------|---|
| отлично | <p>В полном объеме и точно ответил на заданные вопросы, проявил способность к аналитическому осмыслению практического задания, обнаружил знания теоретических основ и умение связать теорию с практикой, правильно употребил терминологию. Ответ структурирован и аргументирован, характеризуется логичным, последовательным изложением, иллюстрирован примерами из практики и ссылками на исследования, содержит собственные наблюдения и мнения.</p> <p>Соответствует критериям в рамках одного билета:</p> <ul style="list-style-type: none"> • Демонстрирует сформированное умение показать сформированность компетенций вопроса государственного экзамена в ответе. • Демонстрирует сформированное знание в области вопросов билета государственного экзамена. • Демонстрирует успешный опыт использования теоретических и практических знаний. |
|---------|---|

4.3. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы с помощью государственного экзамена

Государственный экзамен наряду с требованиями к содержанию дисциплин учитывает общие требования к студентам, предусмотренные СУОС ВО. К государственному экзамену допускаются студенты, завершившие полный курс по образовательной программе и успешно прошедшие все предшествующие аттестационные испытания, предусмотренные учебным планом.

Сдача государственного экзамена проводится на открытом заседании государственной комиссии, состоящих из научно-педагогического персонала ФГБОУ ВО ПГНИУ и лиц, приглашенных из сторонних организаций. СУОС ВО определены требования к 10.05.01 Компьютерная безопасность, которые учтены в настоящей программе государственного экзамена. В соответствии с СУОС ВО по специальности 10.05.01 Компьютерная безопасность предусмотрено, что содержание государственного экзамена устанавливает вуз. Предлагаемая структура программы позволяет осуществить комплексный контроль формирования всех компетенций в полном объеме.

В течение двух недель перед проведением государственного экзамена по включенным в программу дисциплинам проводятся консультации.

Государственный экзамен проводится по билетам, составленным в соответствии с программой государственного экзамена и утвержденным председателем экзаменационной комиссии. Государственный экзамен проводится в устной форме. Сдача государственного экзамена проводится на заседании экзаменационной комиссии с участием не менее двух третей ее состава.

Проведение государственного экзамена начинается в 8.00. Ответы студентов по билетам начинаются в 9.00. Для подготовки к ответу на государственном экзамене студент может использовать время на подготовку, которое не должно превышать 60 минут. Во время подготовки студент может производить записи. Во время подготовки ответа на вопросы экзаменационного билета студент не имеет права использовать никакие дополнительные текстовые материалы (учебники, справочники) или технические средства, в том числе средства связи, калькуляторы, компьютерную технику. Для записей секретарь экзаменационной комиссии предоставляет студентам листы бумаги формата А4, проштампованные «Для служебного пользования». Во время ответа студент может использовать записи, сделанные им при подготовке к ответу. По окончании ответа листы записей сдаются экзаменационной комиссии. Время ответа студента на государственном экзамене не должно превышать 30 минут.

Члены комиссии имеют право задать уточняющие вопросы в ходе ответа студента на вопрос экзаменационного билета. Члены комиссии могут прервать ответ студента на вопрос экзаменационного билета досрочно. После ответа студента на каждый вопрос экзаменационного билета члены экзаменационной комиссии могут задать дополнительные вопросы.

Для сдачи государственного экзамена из состава группы деканатом формируются

подгруппы количеством не более 12 человек в день.

Структура экзаменационного билета состоит из трех вопросов. Количество билетов определяется исходя из количества вопросов, так, чтобы каждый вопрос попал как минимум в один билет. Ознакомление обучаемых с содержанием экзаменационных билетов запрещается. Студенты обязаны готовиться к экзамену, руководствуясь данной программой. На проведение государственного экзамена выделяется время из расчёта не менее десяти дней для подготовки и сдачи (2 недели). Расписание государственного экзамена утверждается деканом факультета и доводится до сведения студентов не позднее, чем за месяц до начала государственной итоговой аттестации.

Ответы студентов на все поставленные вопросы заслушиваются членами государственной экзаменационной комиссии, каждый из которых выставляет частные оценки по отдельным вопросам экзамена и итоговую оценку, являющуюся результирующей по всем вопросам. Оценка знаний студенты на экзамене выводится по частным оценкам ответов на вопросы билета членов комиссии. В случае равного количества голосов мнение председателя является решающим.

Степень сформированности компетенций студентов на экзамене, определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Члены ГЭК оценивают ответ студента на государственном экзамене, исходя из продемонстрированных знаний и умений. Ответ студента оценивается по представленным критериям.

4.4. Учебно-методическое и информационное обеспечение ГИА

4.4.1. Список литературы

1. Таненбаум, Э. Компьютерные сети. / Э. Таненбаум. – СПб.: Питер, 2012. – 955с.
2. Александров П. С. Курс аналитической геометрии и линейной алгебры: учебник для вузов/П. С. Александров.-Санкт-Петербург:Лань,2009, ISBN 978-5-8114-0908-2.-512.-Предм. указ.: с. 505-511
3. Аналитическая геометрия в примерах и задачах: Учебное пособие.-2.-Москва:ООО "Научно-издательский центр ИНФРА-М",2016, ISBN 9785160112022.-496.
4. Кострикин А. И. Введение в алгебру. учебник для студентов университетов по специальности "Математика" и "Прикладная математика" Ч. 1.Основы алгебры/А. И. Кострикин.-Москва:Физматлит,2009, ISBN 978-5-94057-452-1.-1.-Предм. указ.: с. 266-271
5. Бочаров П. П., Печинкин А. В. Теория вероятностей и математическая статистика: учебное пособие для студентов вузов, обучающихся по направлению "Физика", "Прикладная математика и информатика", спец. "Физика", "Прикладная математика"/П. П. Бочаров, А. В. Печинкин.-М.:ФИЗМАТЛИТ,2005, ISBN 5-9221-0633-3.-296.-Библиогр. в конце разд.
6. Гмурман В. Е. Теория вероятностей и математическая статистика: учеб. пособие. - 12-е изд., перераб. - 2011
7. Колемаев В. А. Теория вероятностей и математическая статистика: Учебник для вузов/Колемаев В. А..-Москва:ЮНИТИ-ДАНА,2012, ISBN 5-238-00560-1.-352.
8. Веретенников В. Н. Сборник задач по математике. Введение в математический анализ. Дифференциальное исчисление функций одной переменной/Веретенников В. Н..-Санкт-Петербург: Российский государственный гидрометеорологический университет,2011.-340.
9. Кудрявцев Л. Д. Краткий курс математического анализа. Т. 1. Дифференциальное и интегральное исчисления функций одной переменной. Ряды: Учебник/Л. Д. Кудрявцев.-Москва: Издательская фирма "Физико-математическая литература" (ФИЗМАТЛИТ),2015, ISBN 9785922115858.-444.
10. Ивин А. А. Логика: учебник для студентов вузов/А. А. Ивин.-Москва:Гардарики,2007, ISBN 978-5-8297-0052-2.-352.
11. Морозенко В. В. Дискретная математика: учебное пособие/В. В. Морозенко.-Пермь,2006, ISBN 5-7944-0608-9.-226.-Библиогр.: с. 223-224

12. Балюкевич Э. Л. Дискретная математика: учеб.-практ. пособие / Балюкевич Э.Л., Ковалева Л.Ф., Романников А.Н. - М.: МЭСИ, 2012.
13. Балюкевич Э.Л. Теория информации [Электронный ресурс]: учебное пособие/ Балюкевич Э.Л.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2009.— 215 с.— Режим доступа: <http://www.iprbookshop.ru/10863>.— ЭБС «IPRbooks»
14. Игнатов В.А. Теория информации и передачи сигналов:учебник/В. А. Игнатов.- М.:Радио и связь,1991.-280.
15. Тюрин С. Ф., Аляев Ю. А. Дискретная математика: практическая дискретная математика и математическая логика:учебное пособие для студентов вузов, обучающихся по специальности 210440 "Телекоммуникации"/С. Ф. Тюрин , Ю. А. Аляев.-Москва:Финансы и статистика,2010, ISBN 978-5-279-03463-5.-384.-Библиогр.: с. 382
16. Информатика. Основы информатики. Представление и кодирование информации. Часть 1.Учебное пособие.-Волгоград:Волгоградский институт бизнеса, Вузовское образование,2009.Информатика. Основы информатики. Представление и кодирование информации. Часть 1/Сальникова Н. А..-2009.-94, ISBN 978-5-9061-7215-0
17. Информатика. Часть 1.Учебное пособие.-Краснодар:Южный институт менеджмента,2009.Информатика. Часть 1/Метелица Н. Т..-2009.-114, ISBN 5-93926-041-1
18. Информатика. Часть 2.Учебное пособие.-Краснодар:Южный институт менеджмента,2009.Информатика. Часть 2/Метелица Н. Т..-2009.-99, ISBN 5-93926-041-1
19. Аляев Ю. А., Козлов О. А. Алгоритмизация и языки программирования Pascal, C++, Visual Basic: учебно-справочное пособие для курсантов воен. учеб. заведений и училищ, студентов техн. вузов, учащихся спец. классов школ/Ю. А. Аляев, О. А. Козлов.-М.:Финансы и статистика,2007, ISBN 978-5-279-02294-6.-320.-Библиогр.: с. 318-319
20. Королев Л. Н., Миков А. И. Информатика: введение в компьютерные науки: [учебник для вузов]/Л. Н. Королев, А. И. Миков.-Москва:Высшая школа,2012, ISBN 978-5-4372-0020-9.-3661.-Библиогр.: с. 346-347
21. Городняя Л. В. Основы функционального программирования: учебное пособие/Городняя Л. В..-Москва:Интернет-Университет Информационных Технологий (ИНТУИТ),2016.-246.
22. Залогова Л. А. Основы объектно-ориентированного программирования на базе языка C#:учеб. пособие/Л. А. Залогова.-Санкт-Петербург:Лань,2018
23. Залогова Л. А. Разработка Паскаль-компилятора: учеб. пособие/Л. А. Залогова.-Москва:БИНОМ. Лаборатория знаний,2007, ISBN 978-5-94774-563-4.-183.-Библиогр.: с. 167
24. Алабужев А. А. Архитектура параллельных ЭВМ:учеб.-метод. пособие/А. А. Алабужев.-Пермь:Перм. гос. ун-т,2007, ISBN 5-7944-0928-2.-89.-Библиогр.: с. 79
25. Болдырихин О. В. Гарвардская RISC-архитектура в микроконтроллерах AVR. Средства ввода-вывода, хранения и обработки цифровой и аналоговой информации в микроконтроллерах AVR для построения микропроцессорных систем управления:Методические указания к лабораторной работе по дисциплине "Микропроцессорные системы"/Болдырихин О. В..-Липецк:Липецкий государственный технический университет, ЭБС АСВ,2013.-39.
26. Операционные системы. Часть 1.Учебное пособие.-Томск:Томский государственный университет систем управления и радиоэлектроники,2009.Операционные системы. Часть 1/Гриценко Ю. Б..-2009.-187
27. Операционные системы. Часть 2.Учебное пособие.-Томск:Томский государственный университет систем управления и радиоэлектроники,2009.Операционные системы. Часть 2/Гриценко Ю. Б..-2009.-230
28. Алексеев В.А. Основы проектирования и реализации баз данных [Электронный ресурс]: методические указания к проведению лабораторных работ по курсу «Базы

- данных»/ Алексеев В.А.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2014.— 26 с.— Режим доступа: <http://www.iprbookshop.ru/55122>
29. Богданова А. Л. Базы данных. Теория и практика применения: Учебное пособие/Богданова А. Л.-Химки:Российская международная академия туризма,2010.-125.
30. Карпов А. С. Теоретические основы и практические подходы построения распределенных вычислительных систем: Учебно-методическое пособие/Карпов А. С.-Москва:Российский государственный университет инновационных технологий и предпринимательства,2012, ISBN 978-5-98427-047-2.-48.
31. Лядова Л. Н.,Мызникова Б. И.,Фролова Н. В. Основы информатики и информационных технологий:учеб. пособие для студентов экон. специальностей/Л. Н. Лядова, Б. И. Мызникова, Н. В. Фролова.-Пермь:Перм. гос. ун-т,2007, ISBN 5-7944-1007-8.-311.
32. Грекул В. И. Проектирование информационных систем:учебное пособие/Грекул В. И.-Москва:Интернет-Университет Информационных Технологий (ИНТУИТ),2008, ISBN 5-9556-0033-7.-486.
33. Голиков А. М. Основы информационной безопасности:Учебное пособие/Голиков А. М.-Томск:Томский государственный университет систем управления и радиоэлектроники,2007, ISBN 978-5-86889-467-1.-288.
34. Голуб О.В. Стандартизация, метрология и сертификация [Электронный ресурс]: учебное пособие/ Голуб О.В., Сурков И.В., Позняковский В.М.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2014.— 334 с.— Режим доступа: <http://www.iprbookshop.ru/4151>.— ЭБС «IPRbooks»
35. Сергеев А. Г.,Терегеря В. В. Метрология, стандартизация и сертификация:учебник для бакалавров/А. Г. Сергеев, В. В. Терегеря.-Москва:Юрайт,2012, ISBN 978-5-9916-1454-2.-820.-Библиогр.: с. 815-820
36. Винокуров В. М. Сети связи и системы коммутации:Учебное пособие/Винокуров В. М.-Томск:Томский государственный университет систем управления и радиоэлектроники,2012, ISBN 5-86889-215-1.-304.
37. Голиков А. М. Сети и системы радиосвязи и средства их информационной защиты:Учебное пособие/Голиков А. М.-Томск:Томский государственный университет систем управления и радиоэлектроники,2007, ISBN 978-5-86889-393-3.-392.
38. Денисов В. П. Радиотехнические системы:Учебное пособие/Денисов В. П.-Томск:Томский государственный университет систем управления и радиоэлектроники,2012.-335.
39. Нефедов Е. И. Распространение радиоволн и антенно-фидерные устройства:учебное пособие для вузов/Е. И. Нефедов.-Москва:Академия,2010, ISBN 978-5-7695-6460-4.-3164.-Библиогр.: с. 307-314
40. Раннев Г. Г. Измерительные информационные системы:учебник для студентов вузов, обучающихся по специальности "Информационно-измерительная техника и технология"/Г. Г. Раннев.-Москва:Академия,2010, ISBN 978-5-7695-5979-2.-332.-Библиогр.: с. 324
41. Кловский Д. Д. Теория передачи сигналов:учебник для электротехн. ин-тов связи/Д. Д. Кловский.-М.:Связь,1973.-376.-Библиогр.: с. 369-371 (62 назв.)
42. Системы и сети передачи информации. Часть 1. Системы передачи информации.Учебное пособие.-Санкт-Петербург:Российский государственный гидрометеорологический университет,2008.Системы и сети передачи информации. Часть 1. Системы передачи информации/Чернецова Е. А..-2008.-204, ISBN 978-5-86813-204-9
43. Гаврилов Л. П. Основы электронной коммерции и бизнеса:Учебное пособие/Гаврилов Л. П.-Москва:СОЛОН-ПРЕСС,2009, ISBN 978-5-91359-065-7.-592.
44. Черняк В. З. Бизнес-планирование:Учебное пособие/Черняк В. З.-Москва:ЮНИТИ-ДАНА,2012, ISBN 978-5-238-01812-6.-591.

45. Берлин А. Н. Телекоммуникационные сети и устройства: Учебное пособие/Берлин А. Н..-Москва: БИНОМ. Лаборатория знаний, Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, ISBN 978-5-94774-896-3.-320.
46. Винокуров В. М. Сети связи и системы коммутации: Учебное пособие/Винокуров В. М..-Томск: Томский государственный университет систем управления и радиоэлектроники, 2012, ISBN 5-86889-215-1.-304.
47. Байдачный С. С. NET Framework 2.0. Секреты создания Windows-приложений: учебное пособие/Байдачный С. С..-Москва: СОЛОН-ПРЕСС, 2008, ISBN 5-98003-245-2.-520.
48. Власов Ю. В. Администрирование сетей на платформе MS Windows Server: Учебное пособие/Власов Ю. В..-Москва: БИНОМ. Лаборатория знаний, Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, ISBN 978-5-94774-858-1.-384.
49. Грабауров Владимир Александрович Информационные технологии для менеджеров/Владимир Александрович Грабауров.-М.: Финансы и статистика, 2001, ISBN 5-279-02299-3.-368.
50. Храмцов П. Б. Основы Web-технологий: Учебное пособие/Храмцов П. Б..-Москва: БИНОМ. Лаборатория знаний, Интернет-Университет Информационных Технологий (ИНТУИТ), 2007, ISBN 978-5-9556-0100-7.-374.
51. Сети следующего поколения NGN/под ред. А. В. Рослякова.-Москва: Эко-Трендз, 2008, ISBN 978-5-88405-082-2.-420.-Библиогр.: с. 400-420
52. Чекмарев Ю. В. Локальные вычислительные сети: Учебное пособие/Чекмарев Ю. В..-Москва: ДМК Пресс, 2009, ISBN 978-5-94074-460-3.-200.

4.4.2. Список нормативно-правовых документов

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи».
3. Федеральный закон от 08.08.2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».
4. Федеральный закон от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи».
5. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне».
6. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 9.09.2000 г. № Пр.-1895.
9. Указ Президента Российской Федерации от 17.12.1997 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции Указа Президента Российской Федерации от 10.01.2000 г. № 24.
10. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- И. Указ Президента Российской Федерации от 12 мая 2004 года № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» (в редакции Указов Президента Российской Федерации от 22.03.2005 № 329 и от 03.03.2006 г. № 175).
12. Постановление Правительства Российской Федерации от 03.11.1994 г. № 1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
13. Постановление Правительства Российской Федерации от 26.01.2006 г. № 45 «Об организации лицензирования отдельных видов деятельности».

14. Постановление Правительства Российской Федерации от 15.08.2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».
15. Постановление Правительства Российской Федерации от 27.05.2002 г. № 348 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».
16. «Сборник руководящих документов по защите информации от несанкционированного доступа», Гостех-комиссия России, Москва, 1998 г.
17. ГОСТ Р 50922-96. «Защита информации. Основные термины и определения».
18. ГОСТ Р 51275-99. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
19. Рекомендации по стандартизации Р 50.1.053-2005. «Информационные технологии. Основные термины и определения в области технической защиты информации».
20. ГОСТ Р 51583-2000. «Порядок создания автоматизированных систем в защищенном исполнении».
21. ГОСТ Р 51241-98. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».
22. ГОСТ 12.1.050-86. «Методы измерения шума на рабочих местах».
23. ГОСТ Р ИСО 7498-2-99. «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».
24. ГОСТ 2.114-95. «Единая система конструкторской документации. Технические условия».
25. ГОСТ 2.601-95. «Единая система конструкторской документации. Эксплуатационные документы».
26. ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».
27. ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированных систем».
28. ГОСТ 34.003-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
29. РД Госстандарта СССР 50-682-89. «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения».
30. РД Госстандарта СССР 50-34.698-90. «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».
31. РД Госстандарта СССР 50-680-89. «Методические указания. Автоматизированные системы. Основные положения».
32. ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания».
33. ГОСТ 6.10.4-84. «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники, ЕСКД, ЕСПД и ЕСТД».
34. ГОСТ 28195-89. «Оценка качества программных средств. Общие положения».
35. ГОСТ Р ИСО\МЭК 9126-90. «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению».
36. ГОСТ 2.111-68. «Нормоконтроль».
37. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации».

- 38.РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недеklarированных возможностей», Москва, 1999 г.
39. РД Гостехкомиссии России «Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам», Москва, 2000 г.
40. ГОСТ 13661-92. «Совместимость технических средств электромагнитная. Пассивные помехоподавляющие фильтры и элементы. Методы измерения вносимого затухания».
41. «Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», Гостехко-миссия России, Москва, 2001 г.
42. «Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», Гостехкомиссия России, Москва, 2001 г.
43. «Временная методика оценки защищенности речевой конфиденциальной информации от утечки по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва, 2001 г.
44. «Временная методика оценки защищенности речевой конфиденциальной информации от утечки за счет электроакустических преобразований в вспомогательных технических средствах и системах», Гостехкомиссия России, Москва, 2001 г.
45. ГОСТ Р 51318.22-99. «Совместимость технических средств электромагнитная. Радиопомехи промышленные от оборудования информационных технологий. Нормы и методы испытаний».
- 46.СанПиН. 2.2.2./2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы. Москва, 2003 (действуют с 30.06.03 вместо СанПиН 2.2.2.542-96).
- 47.ГОСТ Р 50948-96. «Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности».
48. ГОСТ Р 50949-96. «Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности».
49. ГОСТ Р 50923-96. «Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения».
- 50.ГОСТ 22505-97. «Совместимость технических средств электромагнитная. Радиопомехи промышленные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы измерений».
- 51.ГОСТ Р 50628-93. «Совместимость электромагнитная машин электронных вычислительных персональных. Устойчивость к электромагнитным помехам. Технические требования и методы испытаний».
- 52.ГОСТ Р 51319-99. «Совместимость технических средств электромагнитная. Приборы для измерения радиопомех. Технические требования и методы испытаний».
53. ГОСТ Р 51320-99. «Совместимость технических средств электромагнитная. Радиопомехи промышленные. Методы испытаний технических средств - источников промышленных радиопомех».
54. «Правила устройства электроустановок (ПУЭ)», 7 издание, Москва, 2002 г.
- 55.Решение Гостехкомиссии России от 14.03.95 г. № 32 «Типовое положение о Совете (Технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам».
56. Решение Гостехкомиссии России от 14.03.95 г. № 32 «Типовое положение о подразделении по защите информации от иностранных технических разведок и от её утечки

по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации».

57. Решение Гостехкомиссии России от 14.03.95 г. № 32 «Типовое положение о подразделении по защите информации от иностранных технических разведок и от её утечки по техническим каналам на предприятии (в учреждении, организации)».

58. Решение Гостехкомиссии России от 03.10.1995 г. № 42 «Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и ее утечки по техническим каналам на объекте».

59. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30.08.2002 г. № 282.

60. ГОСТ Р 50922-96. «Защита информации. Основные термины и определения».

61. ГОСТ Р ИСО 7498-1-99. «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель».

62. ГОСТ Р 6.30-2003. «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».

63. ГОСТ Р 92. «Система сертификации ГОСТ. Основные положения».

64. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005), приказ ФСБ от 9 февраля 2005 г. № 66 (зарегистрировано в Минюсте Российской Федерации 3 марта 2005 г. № 6382).

4.4.3. Базы данных и информационно справочные системы

При освоении дисциплины студентам рекомендуется обращаться к электронным ресурсам, доступ к которым предоставляется ПГНИУ, а также к ресурсам свободного доступа.

При изучении тем, подготовке к занятиям, самостоятельной работе и текущему контролю студенты могут обратиться к различным электронным источникам: электронные библиотечные системы, электронные ресурсы удаленного доступа (на иностранных языках), информационно-справочные системы, а также ресурсы свободного доступа.

Доступ к электронным источникам обеспечивается через научную библиотеку ПГНИУ и сеть университета, доступ к ресурсам свободного доступа обеспечивается через университетскую или личную, домашнюю сеть.

Электронные библиотечные системы

Электронная библиотека ПГНИУ: <https://elis.psu.ru>

Электронно-библиотечная система IPRbooks (ЭБС IPRbooks):
<http://www.iprbookshop.ru>

Научная электронная библиотека eLIBRARY.RU: <https://elibrary.ru>

Национальная электронная библиотека (НЭБ): <https://rusneb.ru>

Электронно-библиотечная система издательства «Лань»: <http://e.lanbook.com/>

Электронные ресурсы удаленного доступа (на иностранных языках)

Web of Science: Поисковая платформа, объединяющая реферативные базы данных публикаций в научных журналах: <http://webofknowledge.com>

Реферативная база данных: <https://www.scopus.com>

Издательство John Wiley & Sons, Inc.: <http://onlinelibrary.wiley.com/Oxford University Press>:

Электронно-библиотечная система «Консультант студента»:
<http://www.studentlibrary.ru>

Антиплагиат. Система автоматической проверки текстов на наличие заимствований из общедоступных сетевых источников: <https://www.antiplagiat.ru/>

Ресурсы свободного доступа

Журнал «Сети и системы связи»: <http://ccc.ru>

Издательство «Открытые системы»: <https://www.osp.ru>

Научный журнал «Информационные технологии и телекоммуникации»: <http://itt.sut.ru>

5. ВКР

5.1. Общая характеристика ВКР

ВКР является частью итоговой государственной аттестации и представляет собой самостоятельное законченное исследование, написанное лично обучающимся под руководством научного руководителя; демонстрирующее уровень подготовленности выпускника к самостоятельной профессиональной деятельности.

Содержание выпускной квалификационной работы должно подтверждать сформированность способности обучающегося использовать знания и способы разрешения проблемных ситуаций, полученные применительно к вопросам организации защиты информации, разработки защищенного программного обеспечения. В ВКР специалиста должно быть продемонстрировано: умение проводить научное и/или практическое исследование, анализ, тестирование, разработку, направленные на решение типовых задач в различных научных и научно-практических областях организации защиты информации, разработки защищенного программного обеспечения (проверка существующих закономерностей; верификации имеющихся гипотез, фактов применительно к различным группам); владение студентом стандартными методами и методиками исследования, навыками обработки и интерпретации результатов; умение обобщать и анализировать фактический материал.

Тематика и темы ВКР должны быть актуальны в научном и практическом аспектах и соответствовать современному состоянию науки и направлениям исследований кафедры информационной безопасности и систем связи ПГНИУ.

ВКР должна показывать уровень теоретической подготовки и навыков практического анализа проблем информационной безопасности в различных сферах деятельности человека, проведения необходимых расчетов по обоснованию формулируемых выводов и разработки мероприятий совершенствования профессиональной деятельности в соответствии с ОП ВО.

По письменному заявлению предоставляется возможность подготовки и защиты ВКР по теме, предложенной студентами, в случае обоснованности целесообразности ее разработки для решения теоретико-эмпирических задач и/или практического применения в соответствующей области профессиональной деятельности и/или на конкретном объекте профессиональной деятельности (п. 32 приказ N 636 от 29.06.2015). После обсуждения и согласования темы с руководителем студент оформляет техническое задание по ВКР. Техническое задание по ВКР утверждается на заседании комиссии, состоящей из руководителя и двух преподавателей кафедры, в течение месяца с начала учебного года. Окончательный список тем ВКР утверждается на заседании кафедры, на Ученом совете факультета не позднее, чем за 6 месяцев до защиты ВКР.

Срок представления законченной выпускной квалификационной работы на кафедру - не менее чем за три недели до даты защиты.

ВКР по программе специалитета 10.05.01 Компьютерная безопасность подлежит рецензированию (п. 35 приказ N 636 от 29.06.2015). Рецензент проводит анализ ВКР и представляет в организацию письменную рецензию на указанную работу (далее – рецензия). В рецензии на работу отмечается: актуальность, полнота и обстоятельность изложения поставленной проблемы, решения выдвинутых целей и задач, эффективность используемых методов, практическая ценность и возможность использования полученных результатов. Рецензент, направляя свое внимание на качество выполненной работы, должен дать прямую оценку выполненной студентом ВКР в соответствии с требованиями СУОС.

Кафедра обеспечивает ознакомление обучающегося с отзывом и рецензией не позднее, чем за 5 календарных дней до дня защиты выпускной квалификационной работы (п. 36 приказ N 636 от 29.06.2015).

5.2. Руководство и консультирование

Руководитель ВКР студента назначается из числа преподавателей выпускающей кафедры (при необходимости консультант (консультанты)).

В обязанности руководителя ВКР студента входит:

- составление задания на ВКР, в том числе определение плана-графика выполнения ВКР и контроль его выполнения;
- рекомендации по подбору и использованию источников по теме ВКР специалиста;
- оказание помощи в разработке структуры (плана) ВКР;
- консультирование студента по вопросам выполнения ВКР специалиста;
- анализ текста ВКР и рекомендации по его доработке;
- оценка степени соответствия ВКР требованиям локальных документов и нормативных актов ФГБОУ ВО ПГНИУ;
- информирование о порядке защиты ВКР специалиста, в том числе предварительной, о требованиях к студенту;
- консультирование (оказание помощи) в подготовке выступления и подборе наглядных материалов к защите, включая предварительную защиту;
- составление письменного отзыва о ВКР.

5.3. Требования к содержанию, объему, структуре и оформлению выпускной квалификационной работы

Выпускные квалификационные работы по специальности 10.05.01 «Компьютерная безопасность» могут быть выполнены по одному из следующих направлений:

1. разработка политики безопасности предприятий;
2. разработка программного обеспечения для организации защиты информации;
3. разработка, модификация, адаптация алгоритмов, методов и методик организации защиты информации;
4. разработка, модификация, адаптация мер безопасности в управлении предприятием.

Выпускная квалификационная работа должна содержать в своем тексте следующие части:

1. введение (краткое описание предметной области, в которой решается задача; краткая постановка задачи; актуальность решения поставленной задачи; возможная новизна в решении поставленной задачи);
2. обзор (литературы, программных, аппаратных средств, методик, алгоритмов и т.д. из предметной области решаемой задачи);
3. полную (точную) постановку задачи;
4. проект решения поставленной задачи;
5. описание реализации предложенного проекта решения задачи;
6. обоснование использованных методов, методик, алгоритмов и т.д.;
7. заключение (краткие итоги решения поставленной в работе задачи).

В зависимости от выбранного направления выполнения выпускной квалификационной работы в ее составе могут быть как добавлены дополнительные содержательные части, так и исключены некоторые из вышеперечисленных.

Для работ, связанных с разработкой политики безопасности предприятий, в тексте выпускной квалификационной работы должны быть отражены следующие составляющие:

1. описание объекта защиты информации;
2. формулировка требований к обеспечению режима безопасности на объекте защиты;
3. юридическое обоснование выдвинутых требований по обеспечению режима безопасности на объекте защиты;
4. экономическое обоснование требований по обеспечению режима безопасности на объекте защиты;
5. описание политики безопасности объекта и мер (регламента) по ее соблюдению на выбранном объекте защиты информации.

Для работ, связанных с разработкой программного обеспечения для организации защиты информации, в тексте выпускной квалификационной работы должны быть отражены:

1. обзор существующих программных систем и комплексов, программно-аппаратных комплексов;
2. проект разрабатываемого программного комплекса или информационной системы;
3. описание реализации программного комплекса (информационной системы);

4. экономическое обоснование целесообразности разработки и внедрения нового программного комплекса (информационной системы);
5. результаты тестирования, испытаний, внедрения нового программного комплекса (информационной системы) на предприятии.

Для работ, связанных с разработкой, модификацией и адаптацией алгоритмов, методов и методик организации защиты информации, в тексте выпускной квалификационной работы должны быть отражены:

1. обзор существующих алгоритмов, методов, методик организации защиты информации в рассматриваемой предметной области;
2. описание проекта разработки новых алгоритмов, методов, методик;
3. формальное обоснование эффективности от внедрения новых алгоритмов, методов, методик организации защиты информации на объекте;
4. описание реализации разработанных алгоритмов, методов, методик;
5. описание результатов тестирования, испытаний, внедрения новых алгоритмов, методов, методик организации защиты информации.

Для работ, связанных с разработкой, модификацией и адаптацией мер безопасности в управлении предприятием, в тексте выпускной квалификационной работы должны быть отражены:

1. обзор существующих методов и методик исследований эффективности защиты информации в сфере управления предприятием;
2. анализ актуальной социально-психологической ситуации с позиции защиты информации и компьютерной безопасности;
3. разработка рекомендаций по противодействию и профилактике негативных явлений в сфере управления человеческим фактором в структуре политики безопасности;
4. формальное обоснование эффективности от внедрения разработанных рекомендаций в систему безопасности предприятия;
5. описание результатов внедрения разработанных рекомендаций в систему безопасности предприятия.

Выпускная квалификационная работа оформляется в виде текста с приложением графиков, таблиц и, при необходимости, элементов документации рабочего проекта для разработанного программно-технического комплекса.

Основной текст отчета должен быть набран шрифтом:

- шрифт - Times New Roman;
- размер кегля – 12 pt,
- межстрочный интервал – 1,5;
- выравнивание абзацев – по ширине;
- первая строка – с отступом.

Выделения в основном тексте набираются курсивом, полужирным шрифтом или полужирным курсивом. Использовать подчеркивание для выделения текста не рекомендуется.

Заголовки различных уровней выделяются полужирным и/или полужирным курсивом. При наборе текста в редакторе Microsoft Word рекомендуется использование стандартных стилей заголовков – Заголовок 1, Заголовок 2 и Заголовок 3, со следующими заменами:

- шрифт - Times New Roman;
- выравнивание заголовков – по центру.

Заголовки должны иметь индивидуальные номера, причем номера заголовков нижних уровней должны включать в себя номера вышестоящих заголовков.

Заголовки нумеруются только цифрами. Использование в номерах разделов отчета слов «Глава», «Часть», «Раздел» и т.п., а также знака параграфа – запрещено.

Заголовкам следующих разделов отчета номера не присваиваются:

- Содержание
- Введение
- Заключение

- Список литературы
- Приложения

Приложения имеют индивидуальную нумерацию с использованием латинских или русских букв – Приложение А, Приложение Б и т.д. Допускается нумерация приложений цифрами.

При включении в текст отчета таблиц следует выполнять следующие правила:

- все таблицы должны быть пронумерованы;
- нумерация таблиц в тексте отчета – сквозная;
- каждая таблица кроме номера должна иметь индивидуальное наименование;
- перед наименованием таблицы и после окончания таблицы в тексте отчета должны находиться пустые строки.

Заголовок (подпись) к таблице указывается перед началом таблицы и оформляется следующим образом:

- шрифт - Times New Roman;
- курсив;
- размер кегля – 12 pt,
- межстрочный интервал – 1,5;
- выравнивание абзацев – по правому краю.

Заголовок таблицы занимает минимум две строки:

- в первой строке указывается слово «Таблица» и номер таблицы;
- во второй строке указывается наименование таблицы.

При включении в текст отчета рисунков следует выполнять следующие правила:

- все рисунки должны быть пронумерованы;
- нумерация рисунков в тексте отчета – сквозная;
- каждый рисунок кроме номера должна иметь индивидуальное наименование;
- перед рисунком и после наименованием рисунка в тексте отчета должны находиться пустые строки.

Заголовок (подпись) к рисунку указывается ниже рисунка и оформляется следующим образом:

- шрифт - Times New Roman;
- курсив;
- размер кегля – 12 pt,
- межстрочный интервал – 1,5;
- выравнивание подписи – по центру.

Формулы вставляются в текст как рисунки без подписи. При этом

- формула должна быть выровнена по центру страницы;
- перед началом формулы и после нее должны быть вставлены пустые строки;
- при необходимости формуле может быть присвоен номер, который указывается справа от формулы в круглых скобках,

после включения формулы в тексте отчета должна быть включена расшифровка обозначений, использованных в формуле.

Содержание отчета размещается на второй странице отчета (непосредственно за титульным листом). При использовании текстового редактора Microsoft Word желательно использовать функцию автоматического формирования содержания.

Список литературы оформляется в соответствии с ГОСТ Р 7.0.5 – 2008

5.4. Процедура защиты ВКР

ВКР передается на выпускающую кафедру для проведения нормоконтроля и принятия окончательного решения о допуске к защите, как правило, не менее чем за 2 недели до дня ее защиты по расписанию. Электронный вариант ВКР до даты защиты отправляется студентом на адрес электронной почты кафедры, затем размещается в системе ЕТИС. В случае, если ВКР студента содержит информацию ограниченного доступа, то она рассматривается

экспертной комиссией ПГНИУ. После вынесения комиссией соответствующего заключения, на ВКР оформляется экспертное заключение. В системе ЕТИС размещается вышеуказанное экспертное заключение на ВКР студента, а ВКР студента получает соответствующий гриф доступа к содержащейся в ней информации и размещается в сейфе хранилища документов Лаборатории информационной безопасности. Ознакомление с текстом работы производится согласно правилам доступа к информации соответствующего уровня доступа, установленного экспертной комиссией при рассмотрении ВКР студента.

При наличии отрицательного отзыва руководителя ВКР студент может защищать свою работу, оценку по результатам защиты ВКР выставляет государственная экзаменационная комиссия (далее ГЭК).

Защита ВКР проводится каждым студентом индивидуально, публично на заседаниях ГЭК в соответствии с графиком защит. В процедуре защиты могут принимать участие (задавать вопросы, вступать в дискуссии, давать оценку работе и характеристику студенту) преподаватели, консультанты, представители организаций, на базе которых была выполнена дипломная работа, и другие желающие при условии, что их участие не затрудняет работу ГЭК.

Во время заседания ГЭК по защите ВКР председатель ГЭК обязаны обеспечить на заседании соблюдение порядка государственной итоговой аттестации и защиты ВКР, спокойную доброжелательную обстановку и соблюдение этических норм.

Защита ВКР происходит на открытом заседании ГЭК в следующей последовательности:

- председатель ГЭК объявляет фамилию, имя, отчество выпускника, зачитывает тему работы;
- выпускник докладывает о результатах ВКР;
- выпускник отвечает на заданные по теме ВКР вопросы членов ГЭК и присутствующих лиц;
- председатель ГЭК зачитывает отзыв научного руководителя (если присутствует научный руководитель, то отзыв зачитывает он сам);
- председатель ГЭК зачитывает отзыв рецензента;
- выпускник отвечает на замечания рецензента.

Для сообщения по содержанию ВКР студенту отводится не более 10 минут. Перед сообщением для каждого члена ГЭК предоставляется раздаточный материал. При защите студентом могут представляться дополнительные материалы, характеризующие научную и практическую ценность выполненной работы (печатные статьи по теме, документы, указывающие на практическое применение результатов работы и т. п.), а также могут использоваться технические средства для презентации материалов ВКР. В докладе следует уделить большее внимание эмпирическому исследованию, показав обоснованность сделанных выводов, а также практическую значимость рекомендаций. Общая продолжительность защиты одной ВКР не должна превышать 30 минут.

По окончании защиты ВКР проводится закрытое заседание ГЭК, на котором на основе открытого голосования большинством голосов определяется оценка по каждой работе.

При оценке ВКР также подлежат оцениванию результаты научно-исследовательской и иной деятельности студента (печатные статьи по теме, документы, указывающие на практическое применение результатов работы и т. п.), соответствующие тематике выпускной квалификационной работы, распечатанные и приложенные к ВКР.

Оценивание происходит в соответствии с показателями и критериями, представленными в п 5.5.

5.5. Критерии оценки результатов защиты выпускной квалификационной работы

5.5.1. Показатели и критерии оценки ОК-компетенций

| Код компетенции | Наименование компетенции | Показатели оценивания | Критерии оценивания | Способ / Средство оценивания |
|-----------------|---|---|---|---|
| ОК-1 | владеть культурой мышления, способность использовать основы философских знаний для формирования мировоззренческой позиции, способность воспринимать, критически оценивать и обобщать новые знания | владение культурой мышления, способностью использовать основы философских знаний для формирования мировоззренческой позиции, способностью воспринимать, критически оценивать и обобщать новые знания | Знать: основы философских знаний для формирования мировоззренческой позиции. Уметь: воспринимать, критически оценивать и обобщать новые знания. Владеть: культурой мышления. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОК-2 | владеть навыками коммуникации, уметь аргументировано и грамотно строить устную и письменную речь на русском языке, способность к общению в социальной и производственной деятельности | владение навыками коммуникации, умение аргументировано и грамотно строить устную и письменную речь на русском языке, способностью к общению в социальной и производственной деятельности | Знать: основы социальной и производственной деятельности. Уметь: аргументировано и грамотно строить устную и письменную речь на русском языке. Владеть: навыками коммуникации. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОК-3 | способность работать самостоятельно и в коллективе, уметь находить и принимать организационно-управленческие решения, оценивать их эффективность | способностью работать самостоятельно и в коллективе, умение находить и принимать организационно-управленческие решения, оценивать их эффективность | Знать: основы самостоятельной и коллективной работы. Уметь: находить и принимать организационно-управленческие решения. Владеть: навыками оценки эффективности организационно-управленческих решений. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОК-4 | критически анализировать и оценивать свой профессиональный и социальный опыт, при необходимости готовность изменить профиль своей профессиональной деятельности, демонстрировать готовность к саморазвитию и самосовершенствованию, повышению профессионального уровня и мастерства | критическим анализом и оценкой своего профессионального и социального опыта, при необходимости готовностью изменить профиль своей профессиональной деятельности, демонстрировать готовность к саморазвитию и самосовершенствованию, повышению | Знать: возможности при необходимости изменить профиль своей профессиональной деятельности. Уметь: критически анализировать и оценивать свой профессиональный и социальный опыт. Владеть: знаниями и опытом саморазвития и самосовершенствования, повышения своего профессионального | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|------|---|--|---|---|
| | | профессионального уровня и мастерства | уровня и мастерства. | |
| ОК-5 | способность применять правовые и этические нормы в своей профессиональной деятельности и оценке ее последствий, знать свои права и способность занимать гражданскую позицию | способностью применять правовые и этические нормы в своей профессиональной деятельности и оценке ее последствий, знание своих права и способностью занимать гражданскую позицию | Знать: свои права. Уметь: занимать гражданскую позицию. Владеть: знаниями и опытом применять правовые и этические нормы в своей профессиональной деятельности и оценке ее последствий. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОК-6 | способность анализировать социально значимые проблемы и процессы | способностью анализировать социально значимые проблемы и процессы | Знать: социально значимые проблемы и процессы. Уметь: анализировать социально значимые проблемы и процессы. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОК-7 | знать и уважать историческое наследие и культурные традиции своей страны, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия, способность анализировать основные этапы и закономерности исторического развития общества | знание и уважение исторического наследия и культурных традиций своей страны, толерантное восприятие социальных, этнических, конфессиональных и культурных различий, способностью анализировать основные этапы и закономерности исторического развития общества | Знать: историческое наследие и культурные традиции своей страны. Уметь: анализировать основные этапы и закономерности исторического развития общества. Владеть: навыками толерантного восприятия социальных, этнических, конфессиональных и культурных различий. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОК-8 | владеть базовой лексикой и грамматикой одного из иностранных языков, основами разговорной речи; способность читать тексты на общеобразовательные и профессиональные темы, передавать их содержание на русском и иностранном языках | владение базовой лексикой и грамматикой одного из иностранных языков, основами разговорной речи; способностью читать тексты на общеобразовательные и профессиональные темы, передавать их содержание на русском и иностранном языках | Знать: родной язык и иностранные языки. Уметь: читать тексты на общеобразовательные и профессиональные темы, передавать их содержание на русском и иностранном языках. Владеть: базовой лексикой и грамматикой одного из иностранных языков, основами разговорной речи. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|--|--|---|---|
| ОК-9 | владеть базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях, способность приобретать новые знания, используя современные информационные технологии | владение базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях, способностью приобретать новые знания, используя современные информационные технологии | Знать: основы информатики. Уметь: приобретать новые знания, используя современные информационные технологии. Владеть: базовыми знаниями в области информатики, навыками использования программных средств и работы в компьютерных сетях. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОК-10 | понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны | понимание сущностей и значения информации в развитии современного общества, соблюдение основных требований информационной безопасности, в том числе защиты государственной тайны | Знать: сущность и значение информации в развитии современного общества. Уметь: соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОК-11 | готовность пользоваться основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий | готовностью пользоваться основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий | Знать: основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий; приемы оказания первой медицинской помощи Уметь: пользоваться основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий. Владеть: навыками использования основных методов защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий; навыками оказания первой медицинской помощи | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|--|--|---|---|
| ОК-12 | понимать и стремиться соблюдать нормы здорового образа жизни, владеть средствами самостоятельного использования методов физического воспитания и укрепления здоровья | понимание и стремление соблюдать нормы здорового образа жизни, владение средствами самостоятельного использования методов физического воспитания и укрепления здоровья | Знать: нормы здорового образа жизни. Уметь: понимать и стремиться соблюдать нормы здорового образа жизни. Владеть: средствами самостоятельного использования методов физического воспитания и укрепления здоровья. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОК-13 | способность использовать основы экономических знаний в различных сферах жизнедеятельности | способностью использовать основы экономических знаний в различных сферах жизнедеятельности | Знать: базовые экономические понятия, экономические показатели, используемые для оценки деятельности предприятий, основы управления рисками. Уметь: решать типичные задачи, связанные с экономическим планированием, оценивать риски, анализировать финансовую и экономическую информацию, необходимую для принятия обоснованных решений. Владеть: методами экономического анализа, прогнозирования, планирования, отбора и принятия оптимальных экономических решений. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

5.5.2. Показатели и критерии оценивания ОПК-компетенций

| Код компетенции | Наименование компетенции | Показатели оценивания | Критерии оценивания | Способ / Средство оценивания |
|-----------------|--|---|--|---|
| ОПК-1 | способность использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с математическими и компьютерными | способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с | Знать: основные факты, концепции, принципы теорий, связанных с математическими и компьютерными науками. Уметь: использовать базовые знания естественных наук, | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|--|---|---|---|
| | науками | математическими и компьютерными науками | математики и информатики, основные факты, концепции, принципы теорий, связанных с математическими и компьютерными науками, в сфере своей деятельности. Владеть: навыками использования базовых знаний естественных наук, математики и информатики, основных фактов, концепций, принципов теорий, связанных с математическими и компьютерными науками. | |
| ОПК-2 | способность создавать, анализировать, реализовывать математические и информационные модели с применением современных вычислительных систем | способностью создавать, анализировать, реализовывать математические и информационные модели с применением современных вычислительных систем | Знать: методы математических и информационных моделей. Уметь: создавать, анализировать, реализовывать математические и информационные модели с применением современных вычислительных систем. Владеть: навыками создания, анализа, реализации математических и информационных моделей с применением современных вычислительных систем. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОПК-3 | способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Знать: основные требования информационной безопасности. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|---|--|---|---|
| | | | информационной безопасности. | |
| ОПК-4 | готовность к участию в проведении научных исследований | готовностью к участию в проведении научных исследований | Знать: теоретические основы проведения научных исследований. Уметь: проводить научные исследования. Владеть: навыками участия в проведении научных исследований. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОПК-5 | способность действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма | готовностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма | Знать: основные положения Конституции Российской Федерации. Уметь: действовать в соответствии с Конституцией Российской Федерации, исполняя свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ОПК-6 | способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства | способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства | Знать: социальную значимость своей будущей профессии, цели и смысл государственной службы. Владеть: высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

5.5.3. Показатели и критерии оценивания ПК-компетенций

| Код компетенции | Наименование компетенции | Показатели оценивания | Критерии оценивания | Способ / Средство оценивания |
|-----------------|---|--|---|---|
| ПК-1 | способность взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий | способностью взаимодействовать и сотрудничать с профессиональными сетевыми сообществами, отслеживать динамику развития выбранных направлений области информационных технологий | Знать: профессиональные сетевые сообщества, способы взаимодействия и сотрудничества с профессиональными сетевыми сообществами. Уметь: отслеживать динамику развития выбранных направлений области информационных технологий. Владеть: навыками взаимодействия и сотрудничества с профессиональными сетевыми сообществами. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-2 | способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем | способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем | Знать: нормативные и методические материалы по методам обеспечения информационной безопасности компьютерных систем. Уметь: осуществлять поиск научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем. Владеть: навыками подбора, изучения и обобщения научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|------|---|--|---|---|
| ПК-3 | способность к анализу и формализации поставленных задач в области информационной безопасности | способностью к анализу и формализации поставленных задач в области информационной безопасности | Знать: основные задачи в области информационной безопасности. Уметь: формализовать поставленные задачи в области информационной безопасности. Владеть: методами анализа поставленных задач в области информационной безопасности. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-4 | способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов области компьютерной безопасности | способностью проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов области компьютерной безопасности | Знать: отечественные и зарубежные стандарты в области компьютерной безопасности. Уметь: проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов области компьютерной безопасности. Владеть: основными методами проведения анализа безопасности компьютерных систем с использованием отечественных и зарубежных стандартов области компьютерной безопасности. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-5 | способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций | способностью осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций | Знать: правила составления аналитических обзоров по различным вопросам. Умеет: составлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем. Владеть: навыками разработки рекомендаций по вопросам обеспечения | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|------|---|--|--|---|
| | | | информационной безопасности компьютерных систем по результатам выполненного анализа. | |
| ПК-6 | способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем | способностью разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем | Знать: правила разработки математических моделей защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. Уметь: разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. Владеть: математическим аппаратом для разработки математических моделей защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-7 | способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований | способностью провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований | Знать: правила обоснования и выбора рациональных решений; уровни обеспечения информационной безопасности. Уметь: выбирать рациональные решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований. Владеть: навыками обоснования и выбора рационального | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|------|--|---|---|---|
| | | | решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований. | |
| ПК-8 | способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов | способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов | Знать: направления создания правовой базы в области информационной безопасности. Уметь: разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов. Владеть: навыками составления нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|--|---|--|---|
| ПК-9 | способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем | способностью проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем | Знать: основы обеспечения информационной безопасности компьютерных систем Уметь: проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем Владеть: методиками анализа проектных решений по обеспечению информационной безопасности компьютерных систем | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-10 | способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах | способностью участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах | Знать: основные составляющие системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, формальные модели политик безопасности, политики управления доступом и информационными потоками в компьютерных системах. Уметь: разрабатывать системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах. Владеть: навыками по разработке | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|--|---|--|---|
| | | | системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, навыками по разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах. | |
| ПК-12 | способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований | способностью участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований | Знать: правила проведения экспериментально-исследовательских работ при аттестации системы защиты информации; требования к системам защиты информации. Уметь: участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований. Владеть: навыками аттестации системы защиты информации с учетом требований. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-13 | способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей | способностью к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей | Знать: уязвимости компьютерных систем. Уметь: проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей. Владеть: методиками проведения экспериментальных исследований компьютерных систем с целью выявления уязвимостей. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|---|--|---|---|
| ПК-14 | способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения | способностью обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения | Знать: основные методы оценки правильности выбранной модели, основные научные методы анализа данных. Уметь: обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения. Владеть: навыками корректного выбора модели решения профессиональной задачи, навыками обработки экспериментальных результатов и сопоставления их с теоретическими данными. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-15 | способность оценивать эффективность системы защиты информации в компьютерных системах | способностью оценивать эффективность системы защиты информации в компьютерных системах | Знать: основные показатели эффективности системы защиты информации в компьютерных системах. Уметь: оценивать эффективность системы защиты информации в компьютерных системах. Владеть: методами оценки эффективности системы защиты информации в компьютерных системах. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|---|--|--|---|
| ПК-16 | способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности | способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности | Знать: способы организации работ малых коллективов исполнителей. Уметь: находить и принимать управленческие решения в сфере профессиональной деятельности. Владеть: навыками организации работы малых коллективов исполнителей. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-17 | способность разрабатывать планы работы первичных подразделений | способностью разрабатывать планы работы первичных подразделений | Знать: способы организации труда первичных подразделений. Уметь: разрабатывать планы работы первичных подразделений. Владеть: навыками по планированию работы первичных подразделений. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-18 | способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы | способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы | Знать: основные способы совершенствования системы управления информационной безопасностью компьютерной системы. Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы. Владеть: навыками по совершенствованию системы управления информационной безопасностью компьютерной системы. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|--|---|--|---|
| ПК-19 | способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем | способностью принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем | Знать: основные функции системы обеспечения информационной безопасности компьютерных систем. Уметь: эксплуатировать системы обеспечения информационной безопасности компьютерных систем. Владеть: навыками принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-20 | способность проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации | способностью проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации | Знать: виды оборудования по защите информации. Уметь: проводить проверку технического состояния, профилактические осмотры, текущий ремонт и регламентные работы на оборудовании по защите информации. Владеть: методами проведения проверки технического состояния, профилактических осмотров, текущего ремонта и регламентных работ на оборудовании по защите информации. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|--|---|--|---|
| ПК-21 | способность принимать участие в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты информации | способностью принимать участие в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты информации | Знать: виды оборудования по защите информации. Уметь: принимать участие в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты информации. Владеть: методами приемки, настройки, регулировки, освоения и восстановления работоспособности оборудования защиты информации. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-22 | способностью использовать нормативные правовые документы в своей профессиональной деятельности | способностью использовать нормативные правовые документы в своей профессиональной деятельности | Знать: существующие нормативные правовые документы в своей профессиональной деятельности. Уметь: использовать нормативные правовые документы в своей профессиональной деятельности. Владеть: навыками использования нормативных правовых документов в своей профессиональной деятельности. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПК-23 | способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами | способностью организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами | Знать: технические и программные средства защиты данных. Уметь: организовать защиту информации техническими и программными средствами. Владеть: приемами антивирусной защиты при работе с компьютерными системами. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

5.5.4. Показатели и критерии оценивания ПСК-компетенций

| Код компетенции | Наименование компетенции | Показатели оценивания | Критерии оценивания | Способ / Средство оценивания |
|-----------------|---|--|---|---|
| ПСК-1 | способность использовать современные методики и технологии программирования для разработки защищенного программного обеспечения | способностью использовать современные методики и технологии программирования для разработки защищенного программного обеспечения | Знать: современные среды разработки программного обеспечения; современные средства тестирования программного обеспечения; способы определения оптимальных средств для разработки программного обеспечения. Уметь: осуществлять внедрение и сопровождение разработанного защищенного программного обеспечения; проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программного обеспечения. Владеть: современными методиками и технологиями программирования для разработки защищенного программного обеспечения. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПСК-2 | способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей | способностью проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей | Знать: правила построения программного обеспечения на различных языках программирования; программные средства для поиска уязвимостей программного обеспечения; способы и средства тестирования программного обеспечения; российский и международные стандарты по разработке программного обеспечения. Уметь: проводить | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|---|--|---|---|
| | | | тестирование программного обеспечения различными средствами. Владеть: навыками поиска уязвимостей в программном обеспечении; навыками проектирования и реализации программного обеспечения в соответствии с требованиями по безопасности программного обеспечения. | |
| ПСК-3 | способность руководствоваться требованиями современных стандартов по безопасности компьютерных систем | способностью руководствоваться требованиями современных стандартов по безопасности компьютерных систем | Знать: российские и международные стандарты по компьютерной безопасности. Уметь: грамотно руководствоваться требованиями современных стандартов по безопасности компьютерных систем. Владеть: навыками применения стандартов безопасности к проектированию и разработке компьютерных систем в соответствии с требованиями к безопасности компьютерных систем. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПСК-4 | способность проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов | способностью проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов | Знать: современные среды разработки программного обеспечения; современные средства тестирования программного обеспечения. Уметь: использовать современные среды разработки программного обеспечения и современные средства тестирования программного обеспечения, проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|-------|---|--|---|---|
| | | | разработки программных продуктов. Владеть: навыками внедрения и сопровождения разработанного программного обеспечения; разработки программного обеспечения в соответствии с существующими технологиями промышленной разработки программного обеспечения. | |
| ПСК-5 | способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах | способностью оценивать эффективность новых образцов программных средств защиты в компьютерных системах | Знать: правила оценки эффективности программных средств защиты; требования к программным средствам защиты компьютерных систем. Уметь: оценивать эффективность новых образцов программных средств защиты в компьютерных системах. Владеть: методиками оценки эффективности программных средств защиты в компьютерных системах. | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |
| ПСК-6 | способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности | способностью применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности | Знать: классификацию и назначение языков и систем программирования, средств прикладного, системного и специального назначения. Уметь: применять современные инструментальные средства программирования для разработки программного обеспечения различного назначения; применять средства прикладного, системного и специального назначения в профессиональной деятельности. Владеть: навыками применения языков, систем и | Защита ВКР (содержание работы, доклад, ответы на вопросы членов государственной комиссии) |

| | | | | |
|--|--|--|---|--|
| | | | инструментальных средств программирования, навыками работы с программными средствами прикладного, системного и специального назначения в профессиональной деятельности. | |
|--|--|--|---|--|

5.5.5. Шкала и критерии оценки защиты выпускной квалификационной работы

| Шкала оценивания | Критерии оценки |
|---------------------|--|
| неудовлетворительно | <p>Работа не соответствует заявленной теме, объекту, предмету исследования, не реализует поставленные цели и не решает указанные задачи, не отвечает требованиям, предъявляемым к выпускным квалификационным работам, в отзыве руководителя имеются серьезные критические замечания, оставшиеся без ответа студента.</p> <p>Актуальность темы - не продемонстрировано. Постановка проблемы – нелогично и непоследовательно сформулирована аппаратная часть исследования (проблема, объект, предмет, цель, задачи, гипотеза, новизна) либо отсутствуют гипотеза/проблема. Анализ литературных источников. В работе отсутствует или приведен поверхностный анализ источников. Рассмотрена одна преобладающая теория или концепция. Не использована иностранная литература. Методология. Не приведены: организация исследования, выборка, методы исследования и математические методы обработки данных. Отсутствуют взаимосвязанные формулировки составляющих методологического аппарата и гипотезы/проблемы. Полученные результаты. Полученные результаты обработаны, отсутствуют интерпретация и обсуждение, сделаны неполные выводы. Выводы не соответствуют цели, задачам и гипотезе(ам) исследования; не имеют теоретическую и практическую значимость. Логика, структура, оформление. В тексте присутствуют не все разделы (титульный лист, содержание, введение, глава 1 – теоретический обзор, глава 2 – организация и методы исследования, глава 3 – результаты исследования и их обсуждение, заключения, список литературы, приложения). Структура не соответствует заявленной теме, нелогична и непоследовательна. Список литературы по большей части состоит из устаревшей литературы. Присутствуют грубые оформительские ошибки. Не расставлены ссылки. Таблицы, рисунки, список литературы оформлены неверно, не в соответствии с ГОСТ. Презентация и ответы на вопросы. Текст доклада (и презентация) не раскрывают тему и проделанную работу. Студент не укладывается в отведенное время (7-10 минут). Не отвечает на вопросы комиссии.</p> <p>Студент не демонстрирует наличие сформированных компетенций:</p> <ul style="list-style-type: none"> • Не демонстрирует опыт сформированности компетенций, полученных при выполнении выпускной квалификационной работы. • Не демонстрирует грамотную речь, неверно использует риторические средства в тексте, несформированное умение осуществлять профессиональное общение. • Не демонстрирует умение продемонстрировать полученные знания и результаты выполнения выпускной квалификационной работы. • Не демонстрирует знание в области задач выпускной квалификационной работы. |
| удовлетворительно | <p>Актуальность темы не подкреплена современными социально-экономическими изменениями, тенденциями развития теории и практики современных систем связи. Постановка проблемы – логично, но непоследовательно сформулирована аппаратная часть исследования (проблема, объект, предмет, цель, задачи, гипотеза, новизна) Анализ литературных источников. Работа содержит аргументированный анализ теоретических положений, соответствующих тематике и проблематике исследования. Рассмотрена одна преобладающая теория или концепция.</p> |

| | |
|--------|--|
| | <p>Использована иностранная литература. Методология. Приведены, но не обоснованы: организация исследования, выборка, методы исследования и математические методы обработки данных. Нарушена взаимосвязь составляющих методологического аппарата и гипотезы/проблемы. Полученные результаты. Полученные результаты обработаны, частично интерпретированы, отсутствует обсуждение, сделаны выводы. Выводы не в полной мере соответствуют цели, задачам и гипотезе(ам) исследования; не указана теоретическая и практическая значимость. Логика, структура, оформление. В тексте присутствуют не все разделы (титальный лист, содержание, введение, глава 1 – теоретический обзор, глава 2 – организация и методы исследования, глава 3 – результаты исследования и их обсуждение, заключения, список литературы, приложения). Структура полностью соответствует заявленной теме, логична и последовательна. Список литературы содержит небольшое количество источников за последние 5-10 лет (общий объем небольшой - 10). Присутствуют оформительские недочеты. Частично представлены соответствующие корректные ссылки. Таблицы, рисунки, список литературы оформлены не в соответствии с ГОСТ. Презентация и ответы на вопросы. Текст доклада (и презентация) слабо раскрывают тему и проделанную работу. Студент не укладывается в отведенное время (7-10 минут). Отвечает на вопросы, не аргументируя собственную позицию.</p> <p>Соответствует сформированным компетенциям в частичном объеме:</p> <ul style="list-style-type: none"> • Демонстрирует фрагментарный опыт сформированности компетенций, полученных при выполнении выпускной квалификационной работы. • Демонстрирует грамотную речь, неверно использует риторические средства в тексте, частично сформированное умение осуществлять профессиональное общение. • Демонстрирует частично сформированное умение продемонстрировать полученные знания и результаты выполнения выпускной квалификационной работы. • Демонстрирует частично сформированное знание в области задач выпускной квалификационной работы. |
| хорошо | <p>Актуальность темы подкреплена современными социально-экономическими изменениями, тенденциями развития теории и практики современной, но не представлены статистические данные. Постановка проблемы – логично и последовательно сформулирована аппаратная часть исследования (проблема, объект, предмет, цель, задачи, гипотеза, новизна), однако имеются нарушения в их взаимосвязях. Анализ литературных источников. Работа содержит аргументированный анализ теоретических положений, соответствующих тематике и проблематике исследования. Рассмотрены основные теории, концепции, подходы, обоснована авторская позиция. Использована иностранная литература. Методология. Аргументированы: организация исследования, выборка, методы исследования и математические методы обработки данных. Нарушена взаимосвязь составляющих методологического аппарата и гипотезы/проблемы. Полученные результаты. Полученные результаты обработаны, проинтерпретированы, не в полной мере обсуждены, сделаны выводы. Выводы соответствуют цели, задачам и гипотезе(ам) исследования; имеют теоретическую и практическую значимость. Логика, структура, оформление. В тексте присутствуют все разделы (титальный лист, содержание, введение, глава 1 – теоретический обзор, глава 2 – организация и методы исследования, глава 3 – результаты исследования и их обсуждение, заключения, список литературы, приложения). Структура полностью соответствует заявленной теме, логична и последовательна. Список литературы содержит источники за последние 5-10 лет (минимум 30). Присутствуют незначительные оформительские недочеты. Присутствуют соответствующие корректные ссылки. Таблицы, рисунки, список литературы оформлены с незначительными отклонениями от ГОСТ. Презентация и ответы на вопросы. Текст доклада (и презентация) логичны, раскрывают тему и проделанную работу. Студент укладывается в отведенное время (7-10 минут). Корректно и обосновано отвечает на вопросы комиссии.</p> <p>Соответствует сформированным компетенциям не в полном объеме:</p> <ul style="list-style-type: none"> • Демонстрирует в целом успешный, но содержащий отдельные пробелы опыт сформированности компетенций, полученных при выполнении выпускной квалификационной работы. • Демонстрирует грамотную речь, неверно использует риторические средства в тексте, сформированное умение осуществлять профессиональное общение. • Демонстрирует сформированное, но содержащее отдельные пробелы умение продемонстрировать полученные знания и результаты выполнения выпускной квалификационной работы. |

| | |
|---------|---|
| | <p>квалификационной работы.</p> <ul style="list-style-type: none"> • Демонстрирует сформированные, но содержащие отдельные пробелы знания в области задач выпускной квалификационной работы. |
| отлично | <p>Актуальность темы подкреплена статистическими данными, современными социально-экономическими изменениями, тенденциями развития теории и практики современных систем связи. Постановка проблемы – логично и обоснованно сформулирована аппаратная часть исследования (проблема, объект, предмет, цель, задачи, гипотеза, новизна). Анализ литературных источников. Работа содержит аргументированный анализ теоретических положений, соответствующих тематике и проблематике исследования. Охвачен широкий спектр теорий, концепций, подходов, обоснована авторская позиция. Использована иностранная литература. Методология. Аргументированы: организация исследования, выборка, методы исследования и математические методы обработки данных. Имеют взаимосвязанные формулировки составляющих методологического аппарата и гипотезы/проблемы.</p> <p>Полученные результаты. Полученные результаты обработаны, проинтерпретированы, обсуждены, сделаны выводы. Выводы соответствуют цели, задачам и гипотезе(ам) исследования; имеют теоретическую и практическую значимость. Логика, структура, оформление. В тексте присутствуют все разделы (титальный лист, содержание, введение, глава 1 – теоретический обзор, глава 2 – организация и методы исследования, глава 3 – результаты исследования и их обсуждение, заключения, список литературы, приложения). Структура полностью соответствует заявленной теме, логична и последовательна. Список литературы содержит источники за последние 5-10 лет (минимум 30). Отсутствуют оформительские ошибки. Присутствуют соответствующие корректные ссылки. Таблицы, рисунки, список литературы оформлены в соответствии с ГОСТ. Презентация и ответы на вопросы. Текст доклада (и презентация) логичны, раскрывают тему и проделанную работу. Студент укладывается в отведенное время (7-10 минут). Корректно и обосновано отвечает на все вопросы комиссии.</p> <p>Соответствует сформированным компетенциям:</p> <ul style="list-style-type: none"> • Демонстрирует сформированный опыт сформированности компетенций, полученных при выполнении выпускной квалификационной работы. • Демонстрирует грамотную речь, использует риторические средства в тексте, сформированное умение осуществлять профессиональное общение. • Демонстрирует сформированное умение продемонстрировать полученные знания и результаты выполнения выпускной квалификационной работы. • Демонстрирует сформированное знание в области задач выпускной квалификационной работы. |

6. Материально-техническое и программное обеспечение государственной итоговой аттестации

Материально-техническая база государственной итоговой аттестации обеспечивается наличием:

а) зданий и помещений, находящихся у ПГНИУ на правах оперативного управления, аренды, оформленных в соответствии с действующими требованиями, где осуществляется индивидуальная аудиторная подготовка студентов по данной дисциплине. Обеспеченность одного обучающегося приведенного к очной форме обучения, общими учебными площадями, соответствует нормативным критериям;

б) фондов и структурных подразделений Научной библиотеки ПГНИУ (для подготовки к занятиям), в т.ч. читальный зал библиотеки ПГНИУ;

в) персональных компьютеров преподавателей и студентов, другой компьютерной техники ПГНИУ, необходимой для выполнения самостоятельной работы, а также организации работы в аудитории;

г) мультимедиа-оборудования для презентации результатов научно-исследовательской работы студентов, демонстрации слайд-презентаций во время доклада;

д) телекоммуникационного оборудования и программных средств, необходимых для реализации ОП и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности.

Перечень необходимых средств, используемых для проведения государственной итоговой аттестации: аудитория для проведения учебных занятий лекционного типа, мультимедийное оборудование, доска.

Перечень используемых информационных технологий: офисное программное обеспечение Microsoft Office (Word, Excel, Power Point). Информационно-справочные и поисковые системы сети Интернет-ресурсы.