Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
И.о. директора института

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
4ae0684d0d529bb9d0248a5b51302ea1
Владелец: Гоконаев Мирослав Валерьевич
Действителен: с 02.08.2024 по 26.10.2025

Фонд оценочных средств
(приложение к рабочей программе модуля)

«РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ	цифровых технологий
РАЗРАБОТЧИК	кафедра информационной безопасности

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

1.1 Результаты освоения дисциплины

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными компетенциями

Код и наименование компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями
ОПК – 8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	Разработка и эксплуатация автоматизированных систем в защищённом исполнении	*Знать:* - Основные информационные технологии, используемые в автоматизированных системах - Виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах - Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем - Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем - Нормативные правовые акты в области защиты информации - Программно-аппаратные средства обеспечения защиты информации в программном обеспечении - Национальные, межгосударственные и международные стандарты в области защиты информации - Методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программного обеспечения - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - Методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программного обеспечения - Программно-аппаратные средства обеспечения защиты информации автоматизированных систем - Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам *Уметь*: - Определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах - Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем - Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите
ОПК –11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем		
ОПК –14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений		

		- Разрабатывать модели угроз безопасности информации и нарушителей в автоматизированных системах - Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите - Определять эффективность применения средств информатизации - Осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений *Владеть навыками:* - проведения технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы - оформления заявки на разработку системы защиты информации автоматизированной системы - разработки компоненты систем защиты информации автоматизированных систем - оформления заявки на разработку системы защиты информации автоматизированной системы - разработки компоненты систем защиты информации автоматизированных систем - разработки отчетных документов и разделов технических заданий - оформления заявки на разработку системы защиты информации- формирования разделов технических заданий на создание систем защиты информации автоматизированных систем - разработки и эксплуатации автоматизированных систем с учётом требований по защите информации

1.2 К оценочным средствам текущего контроля успеваемости относятся:

– тестовые задания открытого и закрытого типа с ключами правильных ответов.

К оценочным средствам для промежуточной аттестации относятся:

- типовые задания по курсовому проекту;

– экзаменационные задания по дисциплине, представленные в виде тестовых заданий закрытого и открытого типов с ключами правильных ответов.

Промежуточная аттестация по дисциплине проводится в форме зачета, который выставляется по результатам прохождения всех видов текущего контроля успеваемости. При необходимости тестовые задания закрытого и открытого типов могут быть использованы для проведения промежуточной аттестации.

1.3 Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (табл. 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно- корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

1.4 Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/ не зачтено («зачтено» – 41-100% правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» - менее 40 % правильных ответов; оценка «удовлетворительно» - от 41 до 60 % правильных ответов; оценка «хорошо» - от 61 до 80% правильных ответов; оценка «отлично» - от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/ не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

Тестовые задания открытого типа:

1. Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации

Эталонный ответ: автоматизированная система в защищенном исполнении (АСЗИ)

2. Защитные меры, эксплуатация которых сокращает степень тяжести последствий нарушения свойств информационной безопасности информационных активов (например, средства резервного копирования и восстановления информации)

Эталонный ответ: апостериорные защитные меры

3. Защитные меры, эксплуатация которых сокращает качественно или количественно существующие уязвимости объектов защиты информационных активов, тем самым снижая

вероятность реализации соответствующих угроз информационной безопасности (например, средства защиты от несанкционированного доступа

Эталонный ответ: априорные защитные меры

4. Состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак

Эталонный ответ: безопасность критической информационной инфраструктуры

5. Единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

Эталонный ответ: государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)

6. Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

Эталонный ответ: информационная система персональных данных

7. Объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

Эталонный ответ: значимый объект критической информационной инфраструктуры

8. Свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки

Эталонный ответ: безотказность

Тестовые задания закрытого типа:

1. Укажите соответствие действий исполнителя при формировании основных документов по результатам исполнения работ на этапе внедрения системы защиты информации:

	Действие		**Документ**
1	Установка и настройка средств защиты информации	а	Акт установки средств защиты информации
2	Внедрение организационных мер, разработка организационно-распорядительных документов	б	Документы по регламентации правил по эксплуатации и вывода из эксплуатации системы защиты информации
3	Выявление и анализ	в	Протокол контроля уязвимостей программного обеспечения и технических средств

4	Испытания и опытная эксплуатация системы защиты информации уязвимостей	г	Протоколы контроля оценки эффективности средств и оценки защищенности информации

Ответ: 1а; 2б; 3в; 4г

2. Укажите последовательность действий исполнителя при проведении аттестации информационных систем по требованиям безопасности информации

1	а	Подача и рассмотрение заявки на аттестацию.
2	б	Предварительное ознакомление с аттестуемым объектом (при необходимости).
3	в	Разработка программы и методики аттестационных испытаний.
4	г	Проведение аттестационных испытаний объекта.
5	д	Оформление, регистрация и выдача аттестата соответствия.

Ответ: 1а; 2б; 3в; 4г; 5д

3. Укажите последовательность действий при создании системы защиты информации

1	а	Формирование требований к системе защиты информации (предпроектный этап).
2	б	Разработка системы защиты информации (этап проектирования).
3	в	Внедрение системы защиты информации (этап установки, настройки, испытаний).
4	г	Подтверждение соответствия системы защиты информации (этап оценки).

Ответ: 1а; 2б; 3в; 4г

ОПК – 11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем

Тестовые задания открытого типа:

1. Наработка —

Эталонный ответ: продолжительность или объем работы объекта.

2. Свойство объекта, заключающееся в приспособленности к поддержанию и восстановлению работоспособного состояния путем технического обслуживания и ремонта

Эталонный ответ: ремонтопригодность.

3. Время, затрачиваемое на восстановление работоспособности объекта -

Эталонный ответ: время восстановления.

4. Свойство объекта сохранять работоспособное состояние до наступления предельного состояния при установленной системе технического обслуживания и ремонта

Эталонный ответ: долговечность

5. Количественная характеристика одного или нескольких единичных свойств, определяющих надежность объекта

Эталонный ответ: показатель надежности

6. Основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

Эталонный ответ: замысел защиты информации.

7. Предохранение вычислительной системы и ее данных от повреждения или потери.

Эталонный ответ: защита вычислительной системы

8. Защищенное средство вычислительной техники (защищенная автоматизированная система) —

Эталонный ответ: средство вычислительной техники (автоматизированная система), в которых реализован комплекс средств защиты.

Тестовые задания закрытого типа:

1. Укажите соответствие действий оператора при администрировании системы защиты информации, выявление инцидентов и реагирование на них, управление конфигурацией объекта и его системой защиты информации, контроль за обеспечение необходимого уровня защищенности информации

1	Заявители	а	осуществляют эксплуатацию объекта информатизации в соответствии с требованиями безопасности информации, а также условиями и ограничениями, установленными эксплуатационной документацией на систему защиты информации, и аттестатом соответствия
2	Заявители	б	извещают орган по аттестации (организацию), выдавший аттестат соответствия, о всех изменениях в информационных технологиях, составе и размещении средств и систем, условиях их эксплуатации, которые могут повлиять на эффективность системы защиты информации
3	Заявители	в	предоставляют необходимые документы и условия для осуществления контроля и надзора за соблюдением порядка аттестации и за эксплуатацией аттестованного объекта информатизации
4	Органы по аттестации	г	Органы по аттестации
5	Органы по аттестации	д	отменяют и приостанавливают действие выданных этим органом (организацией) аттестатов соответствия
6	Органы по аттестации	е	проводят на договорной основе оценку эффективности средств защиты информации и оценку защищенности информации от несанкционированного доступа

Ответ: 1а; 2б; 3в; 4г; 5д; 6е

2. Укажите последовательность действий исполнителя при формировании основных документов по результатам исполнения работ на этапе разработки системы защиты информации

		Документ
1	а	Технический проект (рабочая документация) на создание системы защиты информации
2	б	Описание структуры системы защиты информации.
3	в	Технический паспорт с указанием наименования, состава и мест установки аппаратных и программных средств
4	г	Перечень параметров настройки средств защиты информации.
5	д	Правила эксплуатации средств защиты информации.

Ответ: 1а; 2б; 3в; 4г; 5д

3. Укажите последовательность действий при подаче и рассмотрении заявки на аттестацию объекта информатизации

1	а	Заявителем выбирается исполнитель работ по аттестации объекта информатизации (организация-лицензиат по технической защите конфиденциальной информации)
2	б	Заявителем направляется исполнителю заявка на проведение аттестации с исходными данными на аттестуемый объект
3	в	Исполнителем рассматривается заявка, принимается решение о порядке аттестации, готовятся договорные документы на оказание услуг по аттестации объекта информатизации

Ответ: 1а; 2б; 3в

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

Тестовые задания открытого типа:

1. Защищенное техническое средство обработки информации —

Эталонный ответ: техническое средство обработки информации, удовлетворяющее требованиям нормативно-технических документов по безопасности информации.

2. Защищенные (закрытые) системы и комплексы телекоммуникации —

Эталонный ответ: системы и комплексы телекоммуникации, в которых обеспечивается защита информации с использованием шифровальных средств, защищенного оборудования и организационных мер.

3. Заявитель в области защиты информации —

Эталонный ответ: предприятие, представившее документы, необходимые для получения лицензии или решения о выдаче лицензии

4. Процесс определения, проектирования, разработки, проверки и реализации новой системы, аппаратных средств, программного обеспечения или набора методов и процедур

Эталонный ответ: разработка системы

5. Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники

Эталонный ответ: показатель защищенности средств вычислительной техники.

6. Показатель качества объекта —

Эталонный ответ: мера реализации частной цели объекта, поставленной при его создании (обычно в форме функции).

7. Показатель эффективности объекта —

Эталонный ответ: мера реализации главной цели объекта, поставленной при его создании и определяющей его назначение в условиях целевого применения.

8. Совокупность действий, направленных на разработку и (или) практическое применение способов и средств контроля эффективности защиты информации

Эталонный ответ: мероприятия по контролю эффективности защиты информации

Тестовые задания закрытого типа:

1. Укажите соответствие действий исполнителя при формировании основных документов по результатам исполнения работ на этапе формирования требований к системе защиты информации:

	Действие		**Документ**
1	Принятие решения о необходимости защиты информации	а	Локальный нормативный правовой акт, определяющий необходимость создания системы защиты информации
2	Классификация по требованиям защиты информации (по уровню защищенности информации)	б	Акт классификации по требованиям безопасности информации
3	Определение актуальных угроз безопасности информации	в	Частная модель угроз безопасности информации
4	Определение требований к системе защиты информации	г	ТЗ на создание системы защиты информации с указанием требований к мерам и средствам защиты информации

Ответ: 1а; 2б; 3в; 4г

2. Укажите последовательность действий исполнителя при реагировании на инциденты

1	а	подготовка
2	б	обнаружение
3	в	сдерживание
4	г	исправление
5	д	восстановление
6	е	улучшение

Ответ: 1а; 2б; 3в; 4г; 5д; 6е

3. Укажите последовательность действий исполнителя при формировании основных документов по результатам исполнения работ на этапе внедрения системы защиты информации

1	а	Установка и настройка средств защиты информации
2	б	Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта
3	в	Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
4	г	Испытания и опытная эксплуатации системы защиты информации

Ответ: 1а; 2б; 3в; 4г

3 ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ, КУРСОВУЮ РАБОТУ/КУРСОВОЙ ПРОЕКТ, РАСЧЕТНО-ГРАФИЧЕСКУЮ РАБОТУ

В данном разделе по учебному плану типовые задания на контрольную работу, курсовую работу, расчётно-графическую работу не предусмотрены.

Учебным планом предусмотрен курсовой проект.

Одной из центральных проблем при разработке и эксплуатации автоматизированных систем в защищённом исполнении является проблема обеспечения надежности. Как и многие другие технические системы, имеют в своем составе сложные комплексы технических средств. Поэтому многие вопросы теории и практики надежности автоматизированных систем могут рассматриваться как общетехнические. Вместе с тем специфика автоматизированных систем в защищённом исполнении требует в ряде случаев особого подхода и специальных методов анализа и повышения надежности

Выполнение курсового проекта имеет следующие цели:

– подтверждение теоретических положений, высказанных преподавателем на лекциях;

– ознакомление студента с методами научных исследований;

– изучение компьютерных технологий и приобретение навыков решения задач надежности, которые не могут быть изложены на лекциях.

Основные особенности курсового проекта:

– исследовательский характер всех заданий;

– компьютерные технологии решения задач с использованием универсальных программных средств и программ, разработанных авторами;

– необходимость представления решений в аналитическом, численном и графическом виде;

– наличие в описании каждом проекте примера его выполнения.

Рекомендуется использовать универсальные математические системы.

По каждому выполненному проекту студент представляет отчет, который должен содержать следующие пункты:

–постановка задачи;

–модели и алгоритмы решения задачи;

–краткое изложение методики выполнения работы;

–решение задачи в виде формул, таблиц, графиков;

–анализ полученных результатов и основные выводы.

Задание 1. Определение показателей надежности элементов по опытным данным

Постановка задачи

Дано:

- ✓ N – число элементов, находящихся на испытании;
- ✓ t_i – время исправной работы i-го элемента, $i = 1,2,\ldots,n$;
- ✓ n – число отказавших элементов за время испытания t.

Определить показатели надежности элемента:

- ✓ $\lambda(t)$ – интенсивность отказа как функцию времени;
- ✓ $f(t)$ – плотность распределения времени исправной работы элемента;
- ✓ $w(t)$ – параметр потока отказов как функцию времени.

Решения получить в виде таблиц и графиков. При обработке данных вручную и на компьютере их следует разбить на 10 групп (классов). Подбор подходящего распределения необходимо осуществить для уровня значимости, равного 0,05.

Задание 2. Исследование надежности и риска нерезервированной технической системы

Постановка задачи

Дано:

- ✓ структурная схема системы в виде основного (последовательного в смысле надежности) соединения элементов;
- ✓ n – число элементов системы;
- ✓ λ_i – интенсивность отказа i-го элемента системы, $i = 1,2,\ldots,n$;
- ✓ r_i – риск из-за отказа i-го элемента системы, $i = 1,2,\ldots,n$;
- ✓ R – допустимый риск;
- ✓ T – суммарное время работы системы.

Определить:

- ✓ показатели надежности системы:

• $P_c(t)$ – вероятность безотказной работы системы в течение времени t, а также ее значения при $t = T$ и $t = T_1$;

• T_1 – среднее время безотказной работы системы;

- ✓ $R_c(t)$ – риск системы как функцию времени; значение риска при $t = T$ и $t = T_1$;

Задание 3. Исследование надежности и риска резервированной восстанавливаемой системы

Постановка задачи

Дано:

- ✓ T_c – срок службы (долговечность), лет;
- ✓ t – время непрерывной работы, час;
- ✓ λ – интенсивность отказов, час$^{-1}$;
- ✓ μ – интенсивность восстановления, час$^{-1}$;
- ✓ m – допустимая кратность резервирования;
- ✓ r – риск из-за отказов системы, усл. ед.;
- ✓ $R(t)$ – допустимый риск в течение времени t, усл. ед.

Определить:

- ✓ показатели надежности и риска исходной нерезервированной системы;
- ✓ показатели надежности и риска резервированной системы с заданной кратностью резервирования m;

- ✓ эффективность резервирования и восстановления как средств повышения надежности и снижения риска техники.

Задание 4. Исследование надежности информационной восстанавливаемой системы

Постановка задачи

Дано:

- ✓ информационная система с n обслуживающими органами;
- ✓ P – вероятность того, что заявка в произвольный момент времени t будет принята на обслуживание;
- ✓ λ – интенсивность потока заявок на обслуживание;
- ✓ μ – интенсивность обслуживания заявки.

Определить:

- ✓ число обслуживающих органов n, обеспечивающих заданное значение P;
- ✓ длительность переходных процессов в информационной системе;
- ✓ функции готовности системы $K_г(t)$ для найденных значений n.

Решение задачи выполнить в предположении, что время между заявками и время обслуживания подчиняются экспоненциальному закону.

Задание 5. Исследование свойств структурно резервированных систем при общем резервировании с постоянно включенным резервом

Постановка задачи

Дано:

- ✓ техническая система с основным соединением элементов;
- ✓ n – число элементов системы;
- ✓ λ_i – интенсивность отказа элемента i-го типа, i =1, 2, …, n;
- ✓ t – текущее время работы системы, не превосходящее допустимого времени из условия старения;
- ✓ m – кратность резервирования, $m \leq 4$.

Необходимо:

- ✓ оценить эффективность структурного резервирования как метода повышения надежности;
- ✓ выполнить сравнительный анализ надежности системы при структурном и нагрузочном резервировании;
- ✓ исследовать влияние последействия отказов на эффективность структурного резервирования.

Задание 6. Анализ влияния профилактики на надежность технической системы

Постановка задачи

Дано:

- ✓ закон распределения времени безотказной работы системы и его параметры;
- ✓ закон распределения времени восстанавливаемой системы и его параметры;
- ✓ T_2 – среднее время между очередными профилактиками, в часах;
- ✓ $T_{в2}$ – среднее время проведения профилактик, в часах.

Определить:

- ✓ математическое ожидание T_1 и среднее квадратическое отклонение σ_1 времени безотказной работы системы без профилактики;
- ✓ математическое ожидание $T_{в1}$ и среднее квадратическое отклонение $\sigma_{в1}$ времени восстановления системы без профилактики.

Определить показатели надежности системы без профилактики:

- ✓ $K_{г1}$, T, $T_в$;
- ✓ функцию готовности системы $K_{г1}(t)$;
- ✓ среднее суммарное число отказов системы $M_1(t)$;
- ✓ среднюю суммарную наработку системы $m_1(t)$ за время t.

Определить для системы с профилактикой:

- ✓ коэффициент готовности $K_{гс}(t)$, наработку на отказ $T_с$ и среднее время восстановления $T_{вс}$;
- ✓ зависимость коэффициента готовности системы от частоты профилактики для различных значений времени ее проведения в виде таблицы и графика;
- ✓ оптимальное значение частоты профилактики $T_{2,опт}$, при которой коэффициент готовности системы $K_{гс}$ превышает коэффициент готовности $K_{г1}$ системы без профилактики и имеет при этом наибольшее значение.

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Разработка и эксплуатация автоматизированных систем в защищённом исполнении» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация Безопасность открытых информационных систем).

Разработчик – доцент кафедры «Информационная безопасность» — А.Г. Жестовский.

Фонд оценочных средств рассмотрен и одобрен методической комиссией института цифровых технологий (протокол №5 от 29.08.2024 г).

Председатель методической комиссии  О.С. Витренко