Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

Оценочные материалы
по дисциплине
Программно-аппаратные средства защиты информации

Москва
2023

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Капгер И.В. Идентификатор: R5d33df1e-KapgerIV-059b09ee	И.В. Капгер

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ОПК-3 способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач

2. ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

3. ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

4. ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

5. ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

6. ПСК-2 Способность применять программные средства системного и специального назначения, в том числе для обеспечения безопасносго функционирования объектов энергетики с элементами АСУ ТП

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX» (Отчет)
2. Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64К» (Отчет)
3. Отчет по практической работе №3 Установка и настройка персонального средства криптографической защиты информации «ШИПКА» (Отчет)
4. Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail» (Отчет)

БРС дисциплины

8 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Технологии идентификации, аутентификации, авторизации и управления доступом					
Предмет и задачи программно-аппаратной защиты информации		+			
Средства программно-аппаратной защиты информации		+			
Автоматизированная система		+	+	+	
Идентификация и аутентификация			+	+	
Санкционированный и несанкционированный доступ			+	+	
Разграничение ресурсов в локальных автоматизированных системах			+	+	
Управление доступом при помощи средств защиты информации от несанкционированного доступа			+		
Обеспечение конфиденциальности, целостности и доступности информации					
Контрольные суммы. Целостность в АС					+
Межсетевые экраны					+
Защищенные носители					+
Централизованное управление средствами защиты информации					+
	Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

БРС курсовой работы/проекта

8 семестр

Раздел дисциплины	Веса контрольных мероприятий, %			
	Индекс КМ:	КМ-1	КМ-2	КМ-3
	Срок КМ:	4	8	15
Описание объекта анализа		+		
Описание объекта анализа			+	
Разработка проекта программно-аппаратной защиты ЛВС			+	
Заключение				+
	Вес КМ:	40	40	20

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ОПК-3	ОПК-3(Компетенция)	Знать: основные руководящие правовые, методические, и нормативные документы по программно-аппаратной защите информации Уметь: выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности	Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64К» (Отчет) Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail» (Отчет)
ПК-1	ПК-1(Компетенция)	Знать: основные теоретические сведения: сущность, цели, задачи и принципы программно-аппаратной защиты информации Уметь: устанавливать, настраивать и обслуживать программные , программно-аппаратные	Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX» (Отчет)
ПК-5	ПК-5(Компетенция)	Знать:	Отчет по практической работе №3 Установка и настройка

		основные руководящие правовые, методические, и нормативные требования по оценке защищенности средств программно-аппаратной защиты информации Уметь: выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности	персонального средства криптографической защиты информации «ШИПКА» (Отчет) Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail» (Отчет)
ПК-6	ПК-6(Компетенция)	Знать: перечень, классификацию, принцип действия программно-аппаратных средств защиты информации Уметь: выполнять действия по установке, конфигурированию и настройке программно-аппаратных средств защиты информации	Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64К» (Отчет) Отчет по практической работе №3 Установка и настройка персонального средства криптографической защиты информации «ШИПКА» (Отчет)
ПК-7	ПК-7(Компетенция)	Знать: основные характеристики технических средств защиты информации от несанкционированного доступа	Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64К» (Отчет) Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail» (Отчет)

		Уметь: определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	
ПСК-2	ПСК-2(Компетенция)	Знать: программно-аппаратные средства обеспечения защиты информации автоматизированных систем Уметь: производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе	Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX» (Отчет)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Практическое задание по теме "Установка и настройка средства доверенной загрузки «Аккорд-GX»

Краткое содержание задания:
Установить и настроить средства доверенной загрузки «Аккорд-GX»

Контрольные вопросы/задания:

Знать: основные теоретические сведения: сущность, цели, задачи и принципы программно-аппаратной защиты информации	1.2. Принцип работы средств доверенной загрузки
Знать: программно-аппаратные средства обеспечения защиты информации автоматизированных систем	1.1.Назначение средств доверенной загрузки
Уметь: устанавливать, настраивать и обслуживать программные , программно-аппаратные	1.2. Порядок настройки «Аккорд-GX»
Уметь: производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе	1. 1. 1.Порядок установки «Аккорд-GX»

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-2. Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64К»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Практическое задание по теме «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64К»

Краткое содержание задания:
Установить и настроить средства доверенной загрузки «Аккорд-Win64К»

Контрольные вопросы/задания:

Знать: перечень, классификацию, принцип действия программно-аппаратных средств защиты информации	1.2. Принцип работы и функционал средств доверенной загрузки
Знать: основные характеристики технических средств защиты информации от несанкционированного доступа	1. 1. Характеристика средств сертифицированных ФСТЭК используемых для доверенной загрузки
Уметь: выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности	1.2. Порядок настройки «Аккорд-Win64К»

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-3. Отчет по практической работе №3 Установка и настройка персонального средства криптографической защиты информации «ШИПКА»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Практическое задание по теме "Установка и настройка персонального средства криптографической защиты информации «ШИПКА»"

Краткое содержание задания:
Установить и настроить средства персональной криптографической защиты информации «ШИПКА»

Контрольные вопросы/задания:

Уметь: выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности	1.2. Порядок настройки персонального средства криптографической защиты информации «ШИПКА»
Уметь: выполнять действия по установке, конфигурированию и настройке программно-аппаратных средств защиты информации	1.1.Порядок установки персонального средства криптографической защиты информации «ШИПКА»

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail»

Формы реализации: Письменная работа

Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Практическое задание по теме "Установка и настройка средства криптографической защиты информации «Crypton ArcMail»"

Краткое содержание задания:
Установить и настроить средства криптографической защиты информации «Crypton ArcMail»

Контрольные вопросы/задания:

Знать: основные руководящие правовые, методические, и нормативные документы по программно-аппаратной защите информации	1. 1. Назначение средств криптографической защиты информации «Crypton ArcMail»
Знать: основные руководящие правовые, методические, и нормативные требования по оценке защищенности средств программно-аппаратной защиты информации	1. 2. Принцип работы и функционал средств «Crypton ArcMail»
Уметь: определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	1.2. Порядок настройки персонального средства криптографической защиты информации «Crypton ArcMail»

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Аппаратные средства доверенной загрузки. Этапы доверенной загрузки.
2. Различия между открытым и закрытым ключами.
3. Практическое задание № **1** (Вариант ***A***).

Процедура проведения

Экзамен проводится в письменной форме по билетам согласно программе экзамена

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ОПК-3(Компетенция)

Вопросы, задания

1.Программно-аппаратные средства контроля доступа. Устройства ввода идентификационных признаков. Классификация, характеристика.

Материалы для проверки остаточных знаний

1.1.Какие нормативные документы определяют электромагнитную совместимость средств по ЗИ?

Верный ответ: ГОСТ Р МЭК 61326-1-2014 Оборудование электрическое для измерения, управления и лабораторного применения. Требования электромагнитной совместимости

2. Компетенция/Индикатор: ПК-1(Компетенция)

Вопросы, задания

1.Предмет и задачи программно-аппаратной защиты информации. Основные понятия.
2.Средства криптографической защиты информации. Классификация, характеристика.

Материалы для проверки остаточных знаний

1.2. Порядок использования межсетевых экранов для разделения АС и понижения класса одной из АС.

Верный ответ: При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться. Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса. Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов: при обработке информации с грифом "секретно" - не ниже 3 класса; при обработке информации с грифом "совершенно секретно" - не ниже 2 класса; при обработке информации с грифом "особой важности" - не ниже 1 класса.

3. Компетенция/Индикатор: ПК-5(Компетенция)

Вопросы, задания

1.Средства защиты информации. Классификация, характеристика.

Материалы для проверки остаточных знаний

1.3. Понятие идентификации и аутентификации

Верный ответ: Идентификация – это процесс, при котором происходит определение полномочий субъекта при его допуске в ИС, контролирование установленных полномочий в процессе сеанса работы, регистрация действий и др. Аутентификация (установлением подлинности) - проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

2.4. Программно-аппаратные средства аутентификации: биометрические, пассивные и активные устройства.

Верный ответ: В состав аппаратно-программных СИА входят идентификаторы, устройства ввода-вывода (считыватели, контактные устройства, адаптеры, платы доверенной загрузки, разъемы системной платы и др.) и соответствующее ПО. Идентификаторы предназначены для хранения уникальных идентификационных признаков. Кроме того, они могут хранить и обрабатывать разнообразные конфиденциальные данные. Устройства ввода-вывода и ПО пересылают данные между идентификатором и защищаемым компьютером. На мировом рынке информационной безопасности сегмент ААА стабильно растет. Классификация систем идентификации и аутентификации Современные СИА по виду используемых идентификационных признаков разделяются на электронные, биометрические и комбинированные (рис. 6.6) [74, 75,76]. В электронных системах идентификационные признаки представляются в виде цифрового кода, хранящегося в памяти идентификатора. Такие СИА разрабатываются на базе следующих идентификаторов: О идентификаторы iButton (information button - информационная «таблетка»); О контактные смарт-карты (smart card - интеллектуальная карта); О бесконтактные радиочастотные идентификаторы (RFID-системы); О бесконтактные смарт-карты; О USB-ключи или USB-токсны (token - опознавательный признак, маркер). В биометрических системах идентификационными признаками являются индивидуальные особенности человека, называемые биометрическими характеристиками. В основе идентификации и аутентификации этого типа лежит процедура считывания предъявляемого биометрического признака пользователя и его сравнение с предварительно полученным шаблоном. В зависимости от вида используемых характеристик биометрические системы делятся на статические и динамические. Статическая биометрия (также называемая физиологической) основывается на данных, получаемых из измерений анатомических особенностей человека (отпечатков пальцев, формы кисти руки, узора радужной оболочки глаза, схемы кровеносных сосудов лица, рисунка сетчатки глаза, черт лица, фрагментов генетического кода и др.).

4. Компетенция/Индикатор: ПК-6(Компетенция)

Вопросы, задания

1.Организация хранения паролей в операционных системах ОС MS Windows. База данных учетных записей пользователей и возможные атаки на нее.

2.Обеспечение конфиденциальности электронных документов с применением паролей в MS Office. Анализ уязвимостей системы защиты документов в приложениях MS Office.

Материалы для проверки остаточных знаний

1.5. Порядок аттестации средств обработки конфиденциальной информации после установки на них средств программно-аппаратной защиты.

Верный ответ: Подача заявки аттестующую организацию. Аттестовать по нормам безопасности информации может исключительно лицензиат ФСТЭК в части технической защиты конфиденциальной информации. Когда аттестующий орган получает заявку, он рассматривает ее в течение 30 дней. Если исходные сведения

окажутся недостаточными, предпринимается предварительное ознакомление с объектом. Орган по аттестации составляет программу аттестационных испытаний, в которой указываются сроки и методы проверок, контрольное оборудование, состав комиссии. Документ отправляется на согласование заявителю. Заключается договор на аттестацию. Проводятся аттестационные испытания. По факту проверки составляются протоколы испытаний и заключение, в котором перечисляются выявленные недочеты и даются указания по их устранению. Если объект отвечает установленным нормам, на него выдается аттестат соответствия. При отказе заявитель может подать апелляцию в ФСТЭК. Аттестат действует до 3 лет, это время необходимо сохранять неизменными условия работы с КИ.

5. Компетенция/Индикатор: ПК-7(Компетенция)

Вопросы, задания

1.Основные понятия и определения в сфере информационной безопасности. Угрозы информации. Анализ методов и средств защиты информации.

2.Протоколы аутентификации Windows. Уязвимости доступа к операционным системам MS Windows.

Материалы для проверки остаточных знаний

1.6. Требования по защите информации по оценки защищенности средств программно-аппаратной защиты информации.

Верный ответ: Для ЗП существуют свои требования, которым важно соответствовать. Они касаются и расположения ЗП и обстановки внутри. Например, имеет значение количество окон, батарей и вентиляций, материал стен и двери. Подготовленное ЗП не должно допускать утечки информации по различным каналам. На это и направлены проводимые в ходе аттестации испытания: проверяются акустический, виброакустический, электроакустический каналы утечки. Для охраны данных используются сертифицированные средства защиты информации. Чтобы подготовиться к аттестации ЗП нужно изучить требования, указанные в документах ограниченного доступа. Получить их можно, отправив заявку в ФСТЭК. А вот АС аттестуются по другим правилам, которые зависят от вида системы. Всего их существует 7 типов: информационные системы персональных данных (ИСПДн), государственные информационные системы (ГИС), АС обработки конфиденциальной информации, АС управления технологическими процессами (АСУ ТП), информационные системы общего пользования (ИСОП), критические информационные структуры (КИИ), автоматизированные банковские системы (АБС). Важно правильно категорировать АС, потому что для разных систем требования отличаются и диктуются разными нормативными документами. Основными правилами для эксплуатации любой АС являются ограниченный доступ к сведениям, учет носителей информации, антивирусная защита, подсистема выявления фактов незаконного доступа, использование только разрешенного ПО. Сложность состоит в том, что одна и та же АС может аттестоваться по двум направлениям. Поэтому самостоятельно определить требования к системе не всегда возможно. Другой проблемой при аттестации является разработка внутренней документации. Указания на этот счет могут быть туманны и не точны, а количество требуемых документов – пугающим. Например, для аттестации ИСПДн требуется разработать около 60 документов. Центр безопасности информационных систем поможет в разработке документации и подготовке по требованиям информационной безопасности с последующей аттестацией и гарантией прохождения других проверок.

6. Компетенция/Индикатор: ПСК-2(Компетенция)

Вопросы, задания

1.Понятия идентификации, аутентификации и авторизации. Общие принципы. Задачи протокола аутентификации.

2.Основы биометрического доступа к ресурсам. Обзор биометрических технологий.

Материалы для проверки остаточных знаний

1.7. Требования к целостности в руководящих документах

Верный ответ: - должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом: целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ; целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ; - должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время; - должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД; - должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

Оценка: 2

Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу

Для курсового проекта/работы:

8 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты КП/КР

Курсовой проект должен содержать: - титульный лист; - описание объекта анализа; - описание достоинств и недостатков объекта анализа; - разработка проекта программно-аппаратной защиты ЛВС - заключение. Общих рекомендуемый объем – 10-12 листов. По всем вопросам, возникающим при выполнении задания, студент обращается к преподавателю.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

Оценка: 2
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу