МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждениевысшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой СУиИТ
_____ И.М.Першин
«____» _____ 201_ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

По дисциплине	**Б1.Б.39 ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ**		
Направление подготовки	**10.03.01 Информационная безопасность**		
Направленность (профиль)	Комплексная защита объектов информатизации		
Квалификация выпускника	бакалавр		
Форма обучения	очная		
Год начала обучения	2020		
Изучается в	7 семестре		
	Астр. часов	Акад. часов	
Объем занятий: Итого	108 ч.	144 ч.	4з.е.
В том числе аудиторных	40,5 ч.	54 ч.	
Из них:			
Лекций	13,5 ч.	18 ч.	
Лабораторных работ	27ч.	36 ч.	
Практических занятий	-		
Самостоятельной работы	40,5 ч.	54 ч.	
Экзамен	27 ч.	36 ч.	7 семестр

Дата разработки: «__»_____2020 г.

Предисловие

1. Назначение: для проверки знаний, умений и навыков текущего и промежуточного контроля.
2. Фонд оценочных средств текущего контроля и промежуточной аттестации составлен на основе рабочей программы дисциплины«Программно-аппаратные комплексы защиты объектов информатизации» в соответствии с образовательной программой по направлению подготовки 10.03.01 Информационная безопасность утвержденной на заседании учебно-методического совета ФГАОУ ВО «СКФУ», протокол №__ от «__» _____ 201_ г.

3. Разработчик _____ Ермаков А.С., старший преподаватель кафедры СУиИТ

4. ФОС рассмотрен и утвержден на заседании кафедры систем управления и информационных технологий, протокол №__ от «__» _____ 2020 г.

5. ФОС согласован с выпускающей кафедрой кафедры систем управления и информационных технологий, протокол №__ от «__» _____ 2020 г.

6. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:
Председатель_____ Першин И.М.
_____ Антонов В.Ф.
_____ Сорокин И.Д.

Экспертное заключение: данные оценочные средства соответствуют требованиям федерального государственного образовательного стандарта высшего образования, рекомендуются для использования в учебном процессе.

«__» _____ 2020 г._____И.М.Першин

7. Срок действия ФОС один год.

Паспорт фонда оценочных средств для проведения текущего контроля и промежуточной аттестации

По дисциплине **Б1.Б.39 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) Комплексная защита объектов информатизации

Квалификация выпускника Бакалавр

Форма обучения очная

Год начала обучения 2020

Изучается в 7 семестре

Код оцениваемой компетенции	Этап формирования компетенции (№ темы)	Средства и технологии оценки	Вид контроля, аттестации	Тип контроля, аттестации	Наименование оценочного средства	Количество заданий для каждого уровня, шт.	
						Базовый	Повышенный
ОК-5, ОПК-4, ПК-1, ПСК-2	Темы 1-9	собеседование	текущий	устный	Вопросы для собеседования	48	24
ОК-5, ОПК-4, ПК-1, ПСК-2	Темы 4-8	отчет письменный	текущий	письменный	Темы индивидуальных заданий для письменного отчета	22	14
		экзамен	промежуточный	устный	Вопросы к экзамену	38	27
					Вопросы для проверки уровня знаний	31	10
					Вопросы (задания) для проверки умений и навыков	7	17

Составитель _____ Ермаков А.С.
(подпись)

«__» _____201_ г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждениевысшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой СУиИТ
_____ И.М.Першин
«____» _____ 201_ г.

Вопросы к экзаменупо дисциплине
ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Базовый уровень

Знать

1. Методы и средства ограничения доступа к компонентам ЭВМ
2. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания
3. Защита программных средств от исследования
4. Классификация средств исследования программ
5. Защита программ от несанкционированного копирования
6. Методы, затрудняющие считывание скопированной информации
7. методы, препятствующие использованию скопированной информации
8. Основные функции средств защиты от копирования
9. Основные методы защиты от копирования
10. Методы противодействия динамическим способам снятия защиты программ от копирования
11. Характеристика и классификация компьютерных вирусов
12. Характеристика средств нейтрализации компьютерных вирусов
13. Полностью контролируемые компьютерные системы
14. Основные элементы и средства защиты от несанкционированного доступа
15. Системы защиты информации от несанкционированного доступа
16. Аппаратно-программные средства криптографической защиты информации
17. Комплекс «КРИПТОН-ЗАМОК» для ограничения доступа к компьютеру
18. Система защиты данных CRYPTON SIGMA
19. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания
20. Виды мероприятий по защите информации
21. Современные системы защиты ПЭВМ от несанкционированного доступа к информации
22. Уязвимость компьютерных систем
23. Политика безопасности в компьютерных системах. Оценка защищенности
24. Идентификация пользователей КС-субъектов доступа к данным
25. Идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей
26. Протоколы идентификации с нулевой передачей знаний
27. Схема идентификации Гиллоу-Куискуотера
28. Средства и методы ограничения доступа к файлам
29. Система разграничения доступа к информации в КС

30. Концепция построения систем разграничения доступа
31. Организация доступа к ресурсам КС, обеспечение целостности и доступности информации в КС

Уметь, Владеть

32. Применение программно-аппаратных и технических средств защиты информации на защищаемых объектах
33. Настройка систем защиты информации
34. Участие в эксплуатации систем и средств защиты информации защищаемых объектов
35. Выявление и анализ возможных угроз информационной безопасности объектов
36. Проведение регламентные работ и фиксация отказов средств защиты
37. Проведение регламентных работ по проверке систем защиты информации
38. Подбор и применение программно-аппаратных и технических средства защиты информации

Повышенный уровень

Знать

1. Ведение учета, обработки, хранения, передачи, использование различных носителей конфиденциальной информации
2. Обеспечение техники безопасности при проведении организационно-технических мероприятий
3. Организация и проведение проверок объектов информатизации, подлежащих защите
4. Контроль соблюдения персоналом требований режима защиты информации
5. Оценка качества защиты объекта
6. Организация и технология работы с конфиденциальными документами:
7. Участие в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации
8. Участие в организации и обеспечение технологии ведения делопроизводства с учетом конфиденциальности информации
9. Организация документооборота, в том числе электронного, с учетом конфиденциальности информации
10. Организация архивного хранения конфиденциальных документов
11. Оформление документации по оперативному управлению средствами защиты информации

Уметь, Владеть

12. Учет работ и объектов, подлежащих защите
13. Подготовка отчетной документации, связанной с эксплуатацией средств контроля и защиты информации
14. Документирование хода и результатов служебного расследования
15. Использование нормативных правовых актов, нормативно-методических документов по защите информации
16. Обеспечение информационной и компьютерной безопасности на предприятии
17. Выполнение работ по обслуживанию информационных систем
18. Типы компьютерных сетей предприятия
19. Сетевые операционные системы. Принципы построения компьютерных сетей из компьютеров на базе операционной системы Windows
20. Методы защиты средств вычислительной техники
21. Использование защищенных компьютерных систем
22. Определение и инструментарий новых информационных технологии

23. Нормативные документы по установке, эксплуатации и охране труда при работе с персональным компьютером, периферийным оборудованием и компьютерной оргтехникой: охрана труда, правила внутреннего распорядка, трудовой кодекс, должностная инструкция, требования противопожарной безопасности.
24. Критерии безопасности документооборота. Основные требования к защищенному документообороту.
25. Защита информации, тайна, средства защиты информации.
26. Аппаратные и программные средства для защиты компьютерных систем от НСД.
27. Основные технологии построения защищенных информационных систем.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он знает методы работ по доводке и освоению информационных технологий; методы поддержки работоспособности информационных систем и технологий; Показывает умение выполнять работы по доводке и освоению информационных технологий; поддерживать работоспособность информационных систем и технологий; демонстрирует навыки владения методами работ по освоению информационных технологий; инструментамиподдержки работоспособности информационных систем и технологий.

Оценка «хорошо» выставляется студенту, если он имеет знания и практические навыки применения средств реализации информационных технологий;умеет разрабатыватьвесь спектр средств реализации информационных технологий;Владеет инструментами разработки средств реализации информационных технологий в полной мере.

Оценка «удовлетворительно» выставляется студенту, если знания средств реализации информационных технологий имеются, но практических навыков нет; он умеетразрабатывать отдельные средства реализации информационных технологий и владеет отдельными инструментами разработки средств реализации информационных технологий.

Оценка «неудовлетворительно» выставляется студенту, если отсутствуют знания средств реализации информационных технологий; отсутствует умение разрабатывать средства реализации информационных технологий; студент не владеет инструментами разработки средств реализации информационных технологий.

2. Описание шкалы оценивания

Промежуточная аттестацияв форме **экзамена** предусматривает проведение обязательной экзаменационной процедуры и оценивается 40 баллами из 100. В случае, если рейтинговый балл студента по дисциплине по итогам семестра равен 60, то программой автоматически добавляется 32 премиальных балла и выставляется оценка «отлично» Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **40** (**20**$\leq S_{экз} \leq$**40**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
35 – 40	Отлично
28 – 34	Хорошо
20 – 27	Удовлетворительно

3.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения **экзамена** осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по

образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры в СКФУ.

В экзаменационный билет включаются два вопроса и одно практическое задание.

Для подготовки по билету отводится 30 минут.

При подготовке к ответу студенту предоставляется право пользования справочными таблицами.

При проверке практического задания, оцениваются:

- последовательность и рациональность выполнения;
- точность вычислений;
- знание технологий, использованных в ходе выполнения задания

Составитель _____ Ермаков А.С.

«____»_____201_ г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждениевысшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой СУиИТ
_____ И.М.Першин
«____» _____ 201_ г.

Вопросы для собеседования
по дисциплине
ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ
Базовый уровень

Тема 1. Назначение и возможности аппаратно-программных средств защиты информации.

1. *Предмет защиты.*
2. *Информация общедоступная и ограниченного доступа.*
3. *Категории ценности информации.*
4. *Информация как объект права собственности.*

Тема 2. Комплексный подход к защите информации

1. *Угрозы безопасности информационных систем.*
2. *Классификация угроз безопасности.*
3. *Угрозы преднамеренные и случайные.*
4. *Каналы утечки информации прямые и косвенные.*
5. *Угрозы, обусловленные человеческим Фактором.*
6. *Угрозы, обусловленные техническими средствами.*
7. *Угрозы, обусловленные форс-мажорными обстоятельствами.*
8. *Модель нарушителя.*
9. *Классификация методов и средств защиты информации.*

Тема 3. Применение средств криптографической защиты информации.

1. *Построение аппаратных компонентов криптозащиты данных.*
2. *Защита файлов от изменения.*
3. *Электронная цифровая подпись.*

Тема 4. Применение СЗИ от НСД для организации защищенных компьютерных систем

1. *Дискреционный метод организации разграничения доступа.*
2. *Мандатный метод организации разграничения доступа.*
3. *Контроль целостности информации.*
4. *Имитозащита информации.*
5. *Криптографические методы контроля целостности.*
6. *Защищенные операционные системы.*
7. *Средства защиты программного обеспечения от несанкционированной загрузки.*
8. *ПА защита программ от несанкционированного копирования, пароли и ключи.*
9. *Организация хранения ключей.*

Тема 5. Система защиты корпоративной информации «SecretDisk»**.**

1. *Принцип работы.*
2. *Шифрование.*

Тема 6. Система защиты информации «Secret NET 5.0-C».

1. *Механизм контроля входа в систему с использованием аппаратных средств.*
2. *Механизмы разграничения доступа и защиты ресурсов: – механизм полномочного*

разграничения доступа к объектам файловой системы; – механизм замкнутой программной среды; – механизм шифрования файлов; – механизм разграничения доступа к устройствам компьютера; – механизм затирания информации, удаляемой с дисков компьютера.

Тема 7. Средства организации виртуальных частных сетей

1. *Задачи, решаемые VPN.*
2. *Туннелирование в VPN.*
3. *Уровни защищенных каналов.*
4. *Защита данных на канальном уровне.*
5. *Организация VPN средствами протокола PPTP.*
6. *Установка и настройка VPN.*
7. *Анализ защищенности передаваемой информации.*
8. *Защита данных на сетевом уровне.*
9. *Протокол SKIP.*
10. *Протокол IPSec.*
11. *Организация VPN средствами СЗИ VipNet.*
12. *Настройка сетевых соединений виртуальных машин.*
13. *Установка СЗИ VipNet.*

Тема 8. Организация VPN средствами СЗИ StrongNet.

1. *Организация VPN средствами СЗИ StrongNet.*
2. *Генерация и распространение ключевой информации.*

Тема 9. Организация VPN прикладного уровня средствами протокола S/MIMEи СКЗИ КриптоПро CSP.

1. *Организация почтового обмена.*
2. *Активизация IIS.*
3. *Установка СКЗИ КриптоПро CSP.*
4. *Установка Центра сертификации в ОС WindowsServer.*

Повышенный уровень

Тема 1. Назначение и возможности аппаратно-программных средств защиты информации.

1. *Назначение и задачи в сфере обеспечения информационной безопасности.*
2. *Основные нормативные руководящие документы, касающиеся государственной и коммерческой тайны.*
3. *Международный стандарт безопасности информационных систем ISO 17799.*

Тема 2. Комплексный подход к защите информации

1. *Службы защиты информации.*
2. *Обеспечение, аутентичности субъектов информационного взаимодействия.*
3. *Управление доступом.*
4. *Обеспечение секретности и конфиденциальности информации,*
5. *Обеспечение целостности информации.*

Тема 3. Применение средств криптографической защиты информации.

1. *Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа.*
2. *Необходимые и достаточные функции аппаратных средств криптозащиты*

Тема 4. Применение СЗИ от НСД для организации защищенных компьютерных систем

1. *Защита программ от излучения, защита от отладки, от дизассемблирования, от трассировки по прерываниям.*
2. *Защита информации на машинных носителях.*
3. *Защита остатков информации.*

Тема 5. Система защиты корпоративной информации «SecretDisk».

1. *Ключи шифрования.*

2. *Генерация ключей шифрования.*

Тема 6. Система защиты информации «Secret NET 5.0-C».

1. *Механизмы контроля и регистрации событий: – механизм функционального контроля; – механизм регистрации событий безопасности; – механизм контроля целостности; – механизм контроля аппаратной конфигурации компьютера.*

Тема 7. Средства организации виртуальных частных сетей

1. *Настройка СЗИ VipNet.*
2. *Использование протокола IPSec для защиты сетей.*
3. *Шифрование трафика с использованием протокола IPSec.*
4. *Проверка защиты трафика.*
5. *Настройка политики межсетевого экранирования с использованием протокола IPSec.*

Тема 8. Организация VPN средствами СЗИ StrongNet.

1. *Настройка СЗИ StrongNet.*

Тема 9. Организация VPN прикладного уровня средствами протокола S/MIMEи СКЗИ КриптоПро CSP.

1. *Получение сертификатов открытых ключей.*
2. *Организация защищенного обмена электронной почтой.*

1.Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал; все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; студент анализирует полученные результаты, проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки. При ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

2. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного	Рейтинговый балл (в % от

задания	максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

3.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя собеседование по теме.

Предлагаемые студенту задания позволяют проверить компетенции ОК-5, ОПК-4, ПК-1, ПСК-2. Принципиальные отличия заданий базового уровня от повышенного заключаются в том, что задания базового уровня предполагают наличие знаний и умений в области данных компетенций, в то время, как задания повышенного уровня предназначены для демонстрации полного и всеобъемлющего владения знаниями и навыками в области данных компетенций.

Для подготовки к данному оценочному мероприятию необходимо 30 минут.

При подготовке к ответу студенту предоставляется право пользования справочными таблицами.

При проверке задания оцениваются:

последовательность и рациональность выполнения;

- точность формулировок;
- знания технологий, использованных при подготовке ответа.

Составитель _____ Ермаков А.С.
(подпись)

«__»_____ 201_ г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждениевысшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой СУиИТ
_____ И.М.Першин
«____» _____ 201_ г.

Темы индивидуальных заданий для письменного отчета по дисциплине ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИБазовый уровень

Тема 4. Применение СЗИ от НСД для организации защищенных компьютерных систем

1. Каким образом реализуется система фильтрации трафика в Kerio WinRoute Firewall.
2. Каким образом обеспечивается политика FTP в Kerio WinRoute Firewall.
3. Каким образом обеспечивается защита от вредоносного ПО в Kerio WinRoute Firewall..
4. Назначение VPN-сервера, входящего в состав Kerio WinRoute Firewall.
5. Компоненты виртуальной сети ViPNet.
6. Клиенты и Координаторы виртуальной сети ViPNet.
7. Протокол динамической маршрутизации в сети ViPNet.
8. Инкапсуляция в ПО ViPNet.
9. Соединение узлов в одной маршрутизируемой сети.
10. Подключение координатора через межсетевой экран «Со статической трансляцией адресов».
11. Режим межсетевого экрана «С динамической трансляцией адресов».

Тема 5. Система защиты корпоративной информации «SecretDisk»

1. Ключи шифрования Secret Disk Server.
2. Генерация PIN-кодов и ключей шифрования Secret Disk Server.

Тема 6. Система защиты информации «Secret NET 5.0-C».

1. Агент сервера безопасности (*AGENT*) «Secret NET 5.0-C».
2. Локальная база данных (ЛБД) системы защиты«Secret NET 5.0-C».
3. Подсистема идентификации«Secret NET 5.0-C».
4. Подсистема избирательного управления доступом«Secret NET 5.0-C».
5. Подсистема полномочного управления доступом«Secret NET 5.0-C».

Тема 7. Средства организации виртуальных частных сетей.

1. Политики IPsec, для ограничения передаваемого и принимаемого трафика.
2. Создание политики IPsec с помощью сценария.

Тема 8. Организация VPN средствами СЗИ StrongNet.

1. Генерация и распространение ключевой информации в StrongNet.
2. Настройка СЗИ StrongNet.

Повышенный уровень

Тема 4. . Применение СЗИ от НСД для организации защищенных компьютерных систем**.**

1. Туннелирование IP-трафика открытых ресурсов.
2. Виртуальные адреса в сети ViPNet.

3. Маршрутизация трафика координаторов с несколькими сетевыми интерфейсами.
4. Туннелирование трафика открытых ресурсов на канальном уровне.
5. Политики паролей в СДЗ Dallas Lock.
6. Политики авторизации в СДЗ Dallas Lock.

Тема 5. Система защиты корпоративной информации «SecretDisk»

1. Системы "прозрачного" шифрования данных в Secret Disk Server.
2. Открытый интерфейс Secret Disk Server.

Тема 6. Система защиты информации «Secret NET 5.0-C».

1. Подсистема контроля целостности«Secret NET 5.0-C».
2. Подсистема криптографической защиты«Secret NET 5.0-C».
3. Компонента защиты от загрузки«Secret NET 5.0-C».

Тема 7. Средства организации виртуальных частных сетей

1. Политики IPsec на защите серверов.
2. Применение концепции изолирования доменов.

Тема 8. Организация VPN средствами СЗИ StrongNet.

1. Метод выявления и оценки угроз, уязвимостей, рисков OCTAVE.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал; все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; студент анализирует полученные результаты, проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал,грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки. При ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

2. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)

Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

3.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя защиту отчета по лабораторной работе.

Предлагаемые студенту задания позволяют проверить ОК-5, ОПК-4, ПК-1, ПСК-2.

Принципиальные отличия заданий базового уровня от повышенного заключаются в том, что задания базового уровня предполагают наличие знаний и умений в области данных компетенций, в то время, как задания повышенного уровня предназначены для демонстрации полного и всеобъемлющего владения знаниями и навыками в области данных компетенций.

Составитель _____ Ермаков А.С.
«____»_____20 г.

Оценочный лист

№ п/п	Ф.И.О. студента	Параметры состояния образованности									Итоговый балл
		Предметно-информационная составляющая образованности				Деятельностно-коммуникативная составляющая образованности			Ценностно-ориентационная составляющая образованности		
		Контрольно-методический срез	Общеучебные умения и навыки			Уровень развития устной речи	Умение работать с информацией	Грамотность	Умение использовать полученные знания в повседневной жизни	Уровень адекватности самооценки	
			Умение анализировать	Умение доказывать	Умение делать выводы						
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											