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
«____» _____ 202_ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

По дисциплине	**Б1.Б.37 ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ**		
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	47,25 ч.	63 ч.	
Экзамен	20,25 ч.	27 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«Защита информационных процессов в компьютерных системах» в соответствии с образовательной программой по направлению подготовки 10.03.01 Информационная безопасность утвержденной на заседании учебно-методического совета ФГАОУ ВО «СКФУ», протокол №__ от «__» _____ 202_ г.

3. Разработчик _____ Афанасов В.Х., доцент 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.37 ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ**

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
ОПК-3, ОПК-4, ОПК-7, ПК-7, ПК-8, ПК-9	Темы 1,2,5,6	собеседование	текущий	устный	Вопросы для собеседования	54	35
ОПК-3, ОПК-4, ОПК-7, ПК-7, ПК-8, ПК-9	Темы 2,3,5,6,7	отчет письменный	текущий	письменный	Темы индивидуальных заданий для письменного отчета	25	20
		экзамен	промежуточный	устный	Вопросы к экзамену	28	20
					Вопросы для проверки уровня знаний	23	14
					Вопросы (задания) для проверки умений и навыков	5	6

Составитель _____ Афанасов В.Х.
(подпись)

«__» _____202_ 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
«____» _____ 202_ г.

Вопросы к экзаменупо дисциплине
ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ
Базовый уровень

Знать
1. Основные угрозы информации в компьютерных системах.
2. Особенности построения систем защиты информации в зависимости от источника.
3. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
4. Специфика возникновения угроз в открытых сетях.
5. Особенности защиты информации на узлах компьютерной сети.
6. Системы обнаружения атак. Назначение, основные виды, особенности использования.
7. Использование мониторов безопасности повышения защищённости компьютерной системы.
8. Системные вопросы защиты программ и данных.
9. Политика информационной безопасности. Общая структура документа.
10. Особенности реализации политик безопасности в компьютерных системах.
11. Анализ и управление информационными рисками.
12. Причины возникновения и области ИТ рисков.
13. Методология OCTAVE для анализа и управления информационными рисками.
14. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
15. Система лицензирования и сертификации средств защиты.
16. Аттестация защищенных систем.
17. Структуры в РФ, обеспечивающие лицензирование и сертификацию.
18. Нормативная база и ответственность за защиту информации в компьютерных системах.
19. Руководящий документ Гостехкомиссии по оценке защищенности АС.
20. Американские стандарты по защите информации «Розовая книга».
21. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
22. Европейский стандарт по безопасности. ITSEC. Функциональные требования. Вопросы гарантий и эффективности.
23. 0бщие критерии оценки защищенности информационных технологий (COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции. Профиль защиты.

Уметь, Владеть
24. Определение основных видов объектов защиты.
25. Определение основных видов угроз и способов их реализации.
26. Определение основных способов и средств предотвращения для

каждого вида угроз.
27. Сформулировать основные элементы системы инженерно-технической защиты информации.
28. Сбор данных об информационной системе с помощью средств администрирования

Повышенный уровень

Знать
1. Уязвимости платформы Windows.
2. Переполнение буфера.
3. Сплайсинг функций.
4. Межсетевые экраны. Назначение, основные виды, особенности использования.
5. Виртуальные частные сети. Назначение, основные виды, особенности использования.
6. Организация информационной безопасности в Microsoft SQL Server 2022.
7. Общие схемы и роли в Microsoft SQL Server 2022.
8. Биометрические системы аутентификации пользователей
9. Использования шифрования для повышения защищённости компьютерных систем.
10. Использование криптографического хэширования для контроля целостности программ и данных.
11. Использование межсетевых экранов для защиты информационных процессов.
12. Управление доступом с применением схем и ролей в Microsoft SQL Server 2022.
13. Требования к защите автоматизированных систем от НСД.
14. Сравнение механизмов безопасности СУБД SQL Server и Oracle.

Уметь, Владеть
15. Механизмы защиты баз данных. Разграничение доступа. Механизм ролей.
16. Обеспечение надёжности баз данных.
17. Особенности резервного копирования.
18. Журналирование изменений.
19. Использование представлений и хранимых процедур для обеспечения безопасного доступа в Microsoft SQL Server 2022.
20. Использование средств разграничения доступа для повышения защищённости компьютерных 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; умеетразрабатывать весь спектр средств реализации информационных технологий; Владеетинструментами 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**≤$S_{экз}$≤**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 пользованиясправочными таблицами.

При проверке практического задания, оцениваются:

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

Составитель _____ Афанасов В. Х.

«____»_____202_ 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
«____» _____ 202_ г.

Вопросы для собеседования
по дисциплине
ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ
Базовый уровень

Тема 1. Основные угрозы информации в компьютерных системах

1. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.
2. Неправомерное отключение оборудования или изменение режимов работы устройств и программ**.**
3. Запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.).
4. Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях).
5. Неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной.
6. Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

Тема 2. Виды и характер происхождения угроз

1. Физическое разрушение системы.
2. Отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем.
3. Действия по дезорганизации функционирования системы .
4. Перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений.
5. Перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации.
6. Несанкционированное копирование носителей информации;
7. Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.
8. Чтение информации из областей оперативной памяти, используемых операционной системой.
9. Незаконное получение паролей и других реквизитов разграничения доступа.

Тема 3. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера Система обнаружения вторжений (СОВ).

1. Использование систем обнаружения вторжений.
2. Архитектура СОВ.
3. Способы классификации СОВ.
4. Виды систем обнаружения вторжений.
5. Протокольные СОВ.
6. Сетевая СОВ.

Тема 4. Специфика возникновения угроз в открытых сетях.

1. Традиционная модель атаки "один к одному".
2. Традиционная модель атаки "один ко многим".
3. Распределенные атаки.
4. Удаленное проникновение.
5. Локальное проникновение.
6. Удаленный отказ в обслуживании.
7. Локальный отказ в обслуживании.

Тема 5. Особенности защиты информации на узлах компьютерной сети.

1. Совокупность средств и правил обмена информацией на предприятии.
2. Обеспечение доступа сотрудников предприятия к ресурсам.
3. Особенности архитектуры компьютерных сетей.
4. Особенности обработки информации на физическом, канальном, сетевом и транспортном уровнях.
5. Обеспечение безопасности информационного обмена на физическом уровне модели за счет структуризации физических связей между узлами компьютерной сети.
6. Рекомендации по построению компьютерной сети на физическом уровне.
7. Обеспечение безопасности разделения среды передачи коммуникационными средствами канального уровня.
8. Уязвимость системы разрешения сетевых адресов.

Тема 6. Системные вопросы защиты программ и данных.

1. Политика безопасности в компьютерных системах.
2. Средства разграничения доступа пользователей к ресурсам КС.
3. Проверки подлинности пользователя и противодействия выводу КС из строя.
4. Политика информационной безопасности.
5. Дискретная политика безопасности.

Тема 7. Администрирование серверных систем и приложений

1. Создание и ведение сетевой спецификации.
2. Создание и ведение журнала информационной системы.
3. Создание (при необходимости) схемы сети.
4. Создание и ведение другой документации.
5. Консультирование пользователей.

Тема 8. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации

1. Модель эшелонированной защиты.
2. Уровень информированности, политик и процедур.
3. Уровень физической безопасности.
4. Уровень периметра.

Тема 9.Требования к защите автоматизированных систем от НСД.

1. Физическое разграничение доступа.
2. Логическое управление доступом.
3. Процесс регистрации выполняемых действий.
4. Проверка допустимости и корректности произошедших в системе событий.

Повышенный уровень

Тема 1. Основные угрозы информации в компьютерных системах

1. Проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
2. Игнорирование организационных ограничений (установленных правил) при работе в системе;
3. Вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
4. Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
5. Пересылка данных по ошибочному адресу абонента (устройства);
6. Вод ошибочных данных;

Тема 2. Виды и характер происхождения угроз

1. Несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики.
2. Вскрытие шифров криптозащиты информации.
3. Незаконное подключение к линиям связи с использованием пауз в действиях законного пользователя от его имени.
4. Незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации.

Тема 3. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера Система обнаружения вторжений (СОВ).

1. Основанная на прикладных протоколах СОВ.
2. Узловая СОВ.
3. Гибридная СОВ.
4. Пассивные и активные системы обнаружения вторжений.

Тема 4. Специфика возникновения угроз в открытых сетях

1. Этапы реализации атак.
2. Основной этап реализации атак.
3. Основные механизмы реализации атак.

Тема 5. Особенности защиты информации на узлах компьютерной сети.

1. Разграничение доступа к ресурсам внутри сети предприятия.
2. Использование свойств транспортных протоколов для обеспечения безопасности.
3. Реализация политики защиты средствами транспортного уровня с помощью межсетевых экранов.

Тема 6. Системные вопросы защиты программ и данных.

1. Мандатная (полномочная) политика безопасности.
2. Ролевое управление доступом.
3. Статическое разделение обязанностей.
4. Динамическое разделение обязанностей.

Тема 7. Администрирование серверных систем и приложений

1. Консалтинг и управление процессом модернизации ИС.
2. Профилактическое обслуживание компьютеров.
3. Профилактические работы на сервере.
4. Профилактика и консалтинг с целью предотвращения и предупреждения инцидентов и сокращние потерь и убытков при их возникновении.
5. Устранение возникающих проблем и неисправностей в информационной системе.

Тема 8. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации

1. Внутрисетевой уровень.

2. Уровень узла.
3. Уровень приложения.
4. Уровень данных.

Тема 9.Требования к защите автоматизированных систем от НСД.

1. Права и полномочия доступа.
2. Ограничивающий интерфейс.

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 собеседование по теме.

Предлагаемые студенту задания позволяют проверить компетенции ОПК-3, ОПК-4, ОПК-7, ПК-7, ПК-8, ПК-9. 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 _____ Афанасов В.Х.
(подпись)

«__»_____ 202_ 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
«____» _____ 202_ г.

Темы индивидуальных заданий для письменного отчета по дисциплине
ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Базовый уровень

Тема 4. Специфика возникновения угроз в открытых сетях

1. Каким образом реализуется защита файлов в NTFS?
2. Каким образом обеспечивается сжатие файлов и каталогов в NTFS?
3. Значение понятия «многопоточные файлы» в NTFS.
4. Назначение службы отслеживания связей в NTFS.
5. Значение понятия «квоты дискового пространства» в NTFS.
6. Значение понятия «точки повторной обработки» в NTFS.
7. Каким образом реализуется шифрование файлов в NTFS?
8. Учетные записи пользователей на изолированном компьютере или на компьютере, входящем в рабочую группу.
9. Учетная запись с ограниченными правами.
10. Учетная запись администратора компьютера.

Тема 5. Особенности защиты информации на узлах компьютерной сети

1. Принцип действия EFS.
2. Особенности шифрования EFS.
3. Средства шифрования/дешифрования EFS.
4. Восстановление данных.
5. Средства версионного контроля информационной системы

Тема 6. Системные вопросы защиты программ и данных.

1. Состав программных средств, входящих в систему *PGP*.
2. Создание криптографических ключей с помощью программы *PGPkeys*.
3. Возможность восстановления секретного ключа пользователя при его случайной потере в системе *PGP*.
4. Способы шифрования и расшифрования файлов с помощью функций *Encrypt* и *Decrypt* программы *PGPtools*.

Тема 7. Администрирование серверных систем и приложений.

1. Получение информации о соответствии имен компьютеров IP-адресам.
2. Сбор данных об информационных ресурсах, поддерживаемых на компьютере.

Тема 8. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.

1. Функции программы шифрования файлов *CitadelSafstor*.
2. Доступ к шифрованию (расшифрованию).
3. Различия между методами криптографии и стеганографии.
4. Различия в назначении антивирусных программ-сканеров и программ-мониторов.

Повышенный уровень

Тема 4. . Специфика возникновения угроз в открытых сетях.

1. Определите назначение и ограничения файловой системы CDFS.
2. Определите назначение и ограничения файловой системы UDF.
3. Определите назначение и преимущества файловой системы DFS.
4. Наследование разрешений.
5. Управление доступом к реестру.
6. Политика аудита.
7. События аудита.
8. Управление аудитом.

Тема 5. Особенности защиты информации на узлах компьютерной сети

1. Экранирующий маршрутизатор.
2. Шлюз сеансового уровня.
3. Встроенный межсетевой экран.

Тема 6. Системные вопросы защиты программ и данных.

1. Генерация и хранение ключа симметрического шифрования файла в системе PGP.
2. Доступ к зашифрованному файлу со стороны других пользователей.
3. Способы одновременного шифрования (расшифрования) и получения (проверки) электронной цифровой подписи в системе *PGP.*
4. Способы надежного удаления файлов с конфиденциальной информацией с помощью функции *Wipe* программы *PGPtools.*

Тема 7. Администрирование серверных систем и приложений.

1. Описание действующих разрешений на доступ.
2. Приориты запрещений и разрешений.

Тема 8. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.

1. Обеспечение в системе возможности восстановления зашифрованных файлов при невозможности входа пользователя в систему или при его отсутствии.
2. Средства управления параметрами шифрования конфиденциальных документов.
3. Средства добавления электронной цифровой подписи к документам.

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 компетенции ОПК-3, ОПК-4, ОПК-7, ПК-7, ПК-8, ПК-9.

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 _____ Афанасов В.Х.

«____»_____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.											