МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего 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 и промежуточной аттестации

По дисциплине Безопасность информационных систем
Направление подготовки 09.03.02 Информационные системы и технологии
Профиль Информационные системы и технологии
Квалификация выпускника бакалавр
Форма обучения очная
Учебный план 2020

Объем занятий: Итого	135 ч.	5з.е.
В т.ч. аудиторных	40,5 ч.	
Из них:		
Лекций	13,5 ч.	
Лабораторных занятий	27ч.	
Самостоятельная работа	94,5 ч.	

Зачет с оценкой 7 семестр

Дата разработки:

Предисловие

1. Назначение: Фонд оценочных средств текущего контроля и промежуточной аттестации предназначен для проверки знаний студентов.

2. Разработчик: Ермаков Александр Сергеевич, доцент кафедры систем управления и информационных технологий

3. ФОС рассмотрен и утвержден на заседании кафедры систем управления и информационных технологий Протокол №___ от «___»_____г.

4. Фонд оценочных средств текущего контроля и промежуточной аттестации на основе рабочей программы дисциплины, в соответствии с образовательной программой по направлению подготовки 09.03.02 Информационные системы и технологии УМК ИСТиД (филиала) СКФУ в г. Пятигорске, протокол № от «__»_____г.

5. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:

Председатель: И.М. Першин, зав. кафедрой систем управления и информационных технологий

С.В. Зайцев доцент кафедры систем управления и информационных технологий

С.Н.Русак, доцент кафедры систем управления и информационных технологий

6. Экспертное заключение: ФОС текущего контроля и промежуточной аттестации соответствует СУОС ВО

«____»_____ _____(подпись)

7. Срок действия ФОС _____

Паспорт фонда оценочных средств
для проведения текущего контроля и промежуточной аттестации

По дисциплине Безопасность информационных систем

Направление подготовки 09.03.02 Информационные системы и технологии
Профиль Информационные системы и технологии

Квалификация выпускника бакалавр
Форма обучения очная
Учебный план 2020

Код оцениваемой компетенции (или её части)	Этап формирования компетенции	Тип контроля	Вид контроля	Компонент фонда оценочных средств	Количество элементов, шт.	
					Базовый	Повышен-ный
ОПК-3	1-9	текущий	письменный с помощью технических средств	Темы индивидуальных заданий по лабораторным работам	51	67
ОПК-3	6, 8	текущий	устный	Вопросы для собеседования	64	67

Составитель _____ А.С.Ермаков
(подпись)

«____»_____20 г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего 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 по лабораторным работам по дисциплине «Безопасность информационных систем»

Базовый уровень

Тема 8. Межсетевые экраны. Изучение принципов работы межсетевых экранов

1. Объясните принцип работы межсетевых экранов.
2. Опишите конфигурирование межсетевого экрана Windows.
3. Опишите принципы классификации межсетевых экранов.
4. Что такое профиль брандмауэра, домен, частный, общий.
5. Состояние брандмауэра.
6. Правила для исходящих и входящих соединений.
7. Мастер создания правила для нового исходящего подключения.

Тема 9. Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения вторжений.

1. Что подразумевается под обнаружением вторжений?
2. Назовите два основных типа IDS.
3. Может ли узловая IDS всегда определять успех или неудачу проведения атаки?
4. Может ли узловая IDS предотвращать атаку?
5. Возможно ли противостоять контролеру целостности файлов?
6. Назовите пять этапов реализации системы IDS.
7. Является ли идентификация действий пользователей корректной целью применения IDS?
8. Может ли сетевая IDS предотвращать достижение атаками их целей?
9. Что подразумевается под пассивными ответными действиями?
10. Что подразумевается под активными ответными действиями?

Тема 10. Базовое администрирование и разрешение сетевых проблем с использованием утилит командной строки Windows.

1. Использование базовых команд командной строки windows, применяемых для поиска проблем в сети.
2. Проверка настроек IP. проверка соединения на уровне протоколаIP с использованием команды Ping.
3. Каковы различия в параметрах безопасности систем Windows 7 и Windows 10, если они работают в одной и той же сети?

4. Для чего нужен графический пользовательский интерфейс Local Security Policy (Локальная политика безопасности)?
5. При каких условиях файл, защищенный EFS, будет записываться на диск в незашифрованном виде?
6. К файлам, защищенным EFS, всегда имеют доступ, по крайней мере, два пользователя. Кто эти пользователи?
7. Какие два изменения внесены в Windows 7 в функционирование доверительных взаимоотношений?
8. Если в конфигурации безопасности используется параметр Passwords Must Meet Complexity Requirements (Пароли должны соответствовать требованиям сложности), какие требования предъявляются ко всем паролям?
9. Членом какой группы или групп должна являться учетная запись Guest (Гость)?
10. Какая команда может использоваться для управления конфигурацией безопасности системы Windows 10?

Тема11. Анализ и изучение заголовков различных сетевых пакетов.

1. Анализ различных пакетов такие как TCP, HTTP, ICMP, DNS с использованием Wireshark.
2. Установка Wireshark.
3. Файл с захваченным трафиком.

Тема 12. Сканирование и исследования безопасности сети с помощью сканера Nmap.

1) Какими способами можно задать диапазон сканируемых хостов? Как задать несколько адресов?
2) Какие существуют способы поиска активных (включённых) хостов в сети?
3) Какие способы сканирования портов существуют в Nmap? Какими ключами они задаются?

Тема 13. Методы анализа сетевого трафика с использованием WireShark.

1. Что такое неразборчивый режим сетевой карты?
2. Для чего используется WireShark?
3. Каковы основные элементы интерфейса программы Wireshark? Для чего они нужны?
4. Как задаются условия фильтрации трафика?

Тема 14. Установка и настройка VPN сервера.

1. Что такое VPN? Для чего он используется?
2. Какие виды VPN соединений существуют? Для чего они применяются?
3. Какие порты использует SoftEther Server для входящих подключений?
4. Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
5. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе?

6. Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?
7. Почему процесс реализации VPN представляет собой гораздо большее, чем выбор алгоритма шифрования?
8. Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?

Тема 15. Применение криптографии для безопасности данных. Использование криптостем PGP TrueCrypt.

1. Что такое шифрование?
2. Чем отличается симметричное шифрование от ассиметричного?
3. Что такое хэш-функция? Каковы ее свойства?

Тема 16. Проверка безопасности хоста, выявление ошибок конфигурации. Microsoft Baseline Security.

1. Автоматическое сканирование по заданным шаблонам.
2. Проверка продуктов Microsoft на наличие уязвимостей – Microsot Baseline Security Analyzer.
3. Принципы работы межсетевых экранов.
4. Конфигурирование межсетевого экрана Windows.
5. Классификация.
6. Профиль брандмауэра – домен, частный, общий.

Повышенный уровень

Тема 8. Межсетевые экраны. Изучение принципов работы межсетевых экранов

1. Выделите два основных типа межсетевых экранов.
2. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
3. Является ли один из типов межсетевых экранов более безопасным, нежели другой?
4. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
5. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?
6. Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?
7. Что должен обеспечивать межсетевой экран для проверки состояния?
8. При каком условии межсетевой экран прикладного уровня может называться гибридным?
9. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном?
10. Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

Тема 9. Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения вторжений.

1. Должна ли применяться процедура выполнения ответных действий на инцидент в случае половинчатого IP-сканирования?
2. Почему оповещения о наличии в системе "черных ходов"часто оказываются ложными срабатываниями системы обнаружения вторжений?
3. О чем, как правило, говорит ситуация, при которой за небольшой промежуток времени наблюдается большое число различных атак?
4. Какой тип IDS следует применить в организации для защиты веб-сервера от причинения ущерба?
5. Какой тип системы IDS следует выбрать организации для защиты от атак, если в первую очередь рассматривается вопрос стоимости?
6. Понятие и основные функции системы обнаружения вторжений.
7. Установка Snort.
8. Настройка в режим IDS.
9. Создание пользователя.
10. Конфигурационные файлы и файлы настроек.
11. Установка Barnyard2 для снижения нагрузки на сервер.
12. Установка и настройка PulledPork для задания правил для Snort.
13. Установка Basic Analysisand Security Engine – графического визуализатора.
14. Создание службы из Snort и Barnyard2.
15. Отслеживание действия в сети.
16. Создание своих правил в Snort.

Тема 10. Базовое администрирование и разрешение сетевых проблем с использованием утилит командной строки Windows.

1. Определение маршрута (трассировка) пакетов с использованием команды tracert.
2. Разрешение доменных имен с использованием команды nslookup.
3. Проверка вашей сетевой конфигурации и сетевой статистики командой netstat.
4. Какие два признака могут быть обнаружены в случае проявления атаки "грубой силы", направленной на пароль?
5. Признаком какой активности является большое число неудачных попыток доступа к файлам?
6. Каков наиболее защищенный уровень шифрования для службы Terminal Services?
7. Для чего используются политики ограничения программного обеспечения?
8. Каким образом можно настроить политики ограничения программного обеспечения?
9. Каково назначение групповой политики?
10. Расскажите о доверительных взаимоотношениях в Active Directory.

Тема11. Анализ и изучение заголовков различных сетевых пакетов.

1. Исследование заголовка ARP.
2. Исследование заголовка TCP.
3. Исследование заголовка HTTP.
4. Исследование заголовка ICMP.
5. Исследование заголовка DNS.
6. Исследование заголовка UDP.

Тема 12. Сканирование и исследования безопасности сети с помощью сканера Nmap.

1. Как задать диапазон портов? Как просканировать все порты? Как просканировать UDP порты? Как просканировать порты 21,80,8080?
2. Как с помощью nmap определить операционную систему, установленную на удаленном хосте?
3. Для чего используются ключи –v –O –sV ?
4. Для чего используются ключи –sT –sU –sS -A?

Тема 13. Методы анализа сетевого трафика с использованием WireShark.

1. Как объединить условия фильтрации?
2. Что такое отслеживание соединения? Для чего оно используется?
3. Как извлечь файлы из перехваченного трафика?
4. Как определить какие протоколы используются в перехваченном трафике?

Тема 14. Установка и настройка VPN сервера.

1. Что такое NAT? Для чего он используется?
2. Что такое DHCP? Для чего он используется?
3. Что такое SecureNAT и для чего используется?
4. Можно ли рассматривать использование SSH как реализацию VPN?
5. Почему пользовательские VPN требуют строгой аутентификации?
6. Может ли шифрование полностью защитить данные, передаваемые через VPN.
7. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
8. Пригодны ли межузловые VPN для использования между организациями?

Тема 15. Применение криптографии для безопасности данных. Использование криптостем PGP TrueCrypt.

1. Что такое цифровая подпись? Для чего она используется?
2. Для чего используется приложение VeraCrypt? Какой тип шифрования она использует?
3. Для чего используется приложение GnuPG? Какой тип шифрования она использует?

Тема 16. Проверка безопасности хоста, выявление ошибок конфигурации. Microsoft Baseline Security.

1. Составление сценария сканирования по определенным требованиям.
2. Автоматизация проверки.
3. Состояние брандмауэра.
4. Правила для исходящих и входящих соединений.
5. Мастер создания правила для нового исходящего подключения.

Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если в полном объеме изучен курс данной дисциплины и выполнены практические и лабораторные задания

Оценка «хорошо» выставляется студенту, если достаточно полно изучен курс данной дисциплины и выполнены практические и лабораторные задания

Оценка «удовлетворительно» выставляется студенту, недостаточно если полно изучен курс данной дисциплины и выполнены практические и лабораторные задания

Оценка «неудовлетворительно» выставляется студенту, если отсутствуют знания и практические навыки по данной дисциплине

Оценка зачтено ставится студенту, если он демонстрирует понимание темы и может ответить на вопросы базового уровня.

Оценка не зачтено ставится студенту, если он не может ответить на вопросы базового уровня.

1. **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**

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

Процедура проведения данного оценочного мероприятия включает в себя: дискуссию по приведенным выше вопросам на практическом занятии с участием всей академической группы.

Предлагаемые студенту задания позволяют проверить следующие компетенции:

ОПК-3 .

Вопросы базового уровня позволяют оценить, имеют ли студенты представление об обсуждаемой теме, достаточен ли уровень самостоятельной подготовки к занятию.

Вопросы повышенного уровня позволяют оценить, могут ли студенты решать профессиональные задачи по заданной теме.

При подготовке к ответу студенту предоставляется право пользования конспектом лекций.

При проверке задания оцениваются уровень самостоятельной подготовки к занятию, умение применять полученные знания для решения профессиональных задач.

Составитель _____ А.С.Ермаков

(подпись)

«____»_____20 г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего 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: «Безопасность информационных систем»

Базовый уровень

Тема 1. Основы сетевых технологий и обеспечения безопасности сети.

1. Предмет защиты информации.
2. Объект защиты информации.
3. Защита информации в корпоративных сетях.
4. Основы и цель политики безопасности в компьютерных сетях
5. Управление доступом
6. Идентификация и установление подлинности.
7. Проверка полномочий субъектов на доступ к ресурсам
8. Регистрация обращений к защищаемым ресурсам
9. Реагирование на несанкционированные действия
10. Многоуровневая защита корпоративных сетей
11. Аутентификация
12. Анализ возможностей маршрутизации и прокси-серверов

Тема 2. Возможные уязвимости, угрозы и атаки на информационные системы

1. Угроза, уязвимость, атака.
2. Классификация уязвимостей.
3. Источники возникновения уязвимостей
4. Угрозы безопасности в информационно-вычислительных системах.
5. Классификация угроз информационной безопасности.
6. Классификация злоумышленников в сфере компьютерных сетей.
7. Основные методы реализации угроз информационной безопасности в компьютерных сетях.

Тема 3. Классификация атак по уровням иерархической модели OSI.

1. Уровни модели OSI.
2. Атаки на физическом уровне и защита от них.
3. Фрагментация данных.
4. Атака Pingflooding.

5. Нестандартные протоколы, инкапсулированные в IP.
6. Атака smurf. Атака DNS spoofing.
7. Атака IP spoofing.
8. Навязывание пакетов.
9. Sniffing — прослушивание канала.

Тема 4. Мониторинг и анализ трафика в сети.

1. Обзор методов анализа и мониторинга сетевого трафика.
2. Важность мониторинга и анализа сети.
3. Способы мониторинга и анализа.
4. Методы мониторинга, основанные на маршрутизаторе.
5. Протокол простого сетевого мониторинга,
6. Удалённый мониторинг,
7. Netflow.

Тема 5. Атаки на беспроводные устройства и защита от них.

1. Организация сетей Wi-Fi .
2. Угрозы.
3. Прямые угрозы.
4. Чужаки.
5. Нефиксированная природа связи.
6. Уязвимости сетей и устройств.
7. Некорректно сконфигурированные точки доступа.
8. Некорректно сконфигурированные беспроводные клиенты.
9. Взлом шифрования.

Тема 6. Основные типы уязвимостей информационных систем. Защита от уязвимостей.

1. Классификация уязвимостей: технологические, организационные.
2. Эксплуатационные уязвимости.
3. Типовые уязвимости: Неподдерживаемые версии операционных систем и системного программного обеспечения,
4. Уязвимости веб-серверов.

Тема 7. Атаки в виртуальной среде и защита от них.

1. Разведка.
2. Атаки на сети с WEP-шифрованием.
3. Пассивные сетевые атаки.
4. Активные сетевые атаки.
5. Повторное использование вектора инициализации (Initialization Vector Replay Attacks).
6. Манипуляция битами (Bit-Flipping Attacks).

Тема 8. Межсетевые экраны. Изучение принципов работы межсетевых экранов

1. Методы анализа сетевой информации,
2. Статистический метод,
3. Экспертные системы,
4. Нейронные сети.
5. Межсетевые экраны: Назначение, История,

6. Фильтрация трафика,
7. Классификация межсетевых экранов.

Тема 9. Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения вторжений.

1. Система обнаружения вторжений,
2. Виды систем обнаружения вторжений,
3. История разработок СОВ.

Повышенный уровень

Тема 1. Основы сетевых технологий и обеспечения безопасности сети.

1. Причины, виды и каналы утечки информации.
2. Методы и средства защиты информации в информационно-вычислительных системах.
3. Правовые и организационные методы защиты информации в компьютерных сетях.
4. Законодательная база в области информационных технологий
5. Действующие стандарты и рекомендации в области информационной безопасности компьютерных сетей.
6. Защита компьютерной информации в локальных ЭВМ и информационно-вычислительных сетях
7. Модели безопасности основных операционных систем
8. Механизмы защиты операционных систем
9. Система безопасности ОС Windows
10. Защита в операционной системе Unix
11. Системы защиты программного обеспечения.
12. Классификация систем защиты программного обеспечения
13. достоинства и недостатки основных систем защиты
14. Упаковщики/шифраторы
15. Системы защиты от несанкционированного копирования
16. системы защиты от несанкционированного доступа
17. Показатели эффективности систем защиты.

Тема 2. Возможные уязвимости, угрозы и атаки на информационные системы

1. Классификация уязвимостей по уровню в инфраструктуре АС,
2. Классификация уязвимостей по степени риска,
3. CommonVulnera bilitiesand Exposures,
4. Классификация атак по целям,
5. Классификация атак по мотивации действий,
6. Местонахождение нарушителя,
7. Механизмы реализации атак,
8. Статистика по уязвимостям и атакам,
9. Примеры реализации атак.

Тема 3. Классификация атак по уровням иерархической модели OSI.

1. Перехват пакетов на маршрутизаторе.
2. Навязывание хосту ложного маршрута с помощью протокола ICMP.

3. WinNuke.
4. Подмена доверенного хоста.
5. Технологии обнаружения атак.

Тема 4. Мониторинг и анализ трафика в сети.

1. Технологии не основанные на маршрутизаторах,
2. Активный мониторинг,
3. Пассивный мониторинг,
4. Комбинированный мониторинг,
5. Просмотр ресурсов на концах сети,
6. Сетевой монитор с собственной конфигурацией,
7. Атакуемые сетевые компоненты: Сервера, Рабочие станции,
8. Атакуемые сетевые компоненты: Среда передачи информации, Узлы коммутации сетей.

Тема 5. Атаки на беспроводные устройства и защита от них.

1. Имперсонация и Identity Theft.
2. Отказы в обслуживании.
3. Косвенные угрозы.
4. Утечки информации из проводной сети.
5. Особенности функционирования беспроводных сетей.
6. Методы ограничения доступа.
7. Методы аутентификации .
8. Методы шифрования.
9. Атаки на сети wi-fi.

Тема 6. Основные типы уязвимостей информационных систем. Защита от уязвимостей.

1. Использование небезопасных протоколов управления,
2. Использование небезопасных протоколов SSL и TLS,
3. Слабые пароли WPA/WPA2-PSK,
4. Использование протокола разрешения имен NetBIOS по TCP/IP,
5. Межсайтовый скриптинг.
6. Устранение выявленных уязвимостей.

Тема 7. Атаки в виртуальной среде и защита от них.

1. Атаки на сети с WPA/WPA2-шифрованием.
2. Атака по словарю на WPA/WPA2 PSK.
3. Атака переустановки ключа в WPA и WPA2 (KRACK)

Тема 8. Межсетевые экраны. Изучение принципов работы межсетевых экранов

1. Управляемые коммутаторы,
2. Пакетные фильтры,
3. Шлюзы сеансового уровня,
4. Посредники прикладного уровня,
5. Инспекторы состояния,
6. Реализация,
7. Ограниченность анализа межсетевого экрана.

Тема 9. Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения вторжений.

1. Пассивные и активные системы обнаружения вторжений,
2. Сравнение СОВ и межсетевого экрана.
3. Установка и конфигурирование СОВ.

Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если в полном объеме изучен курс данной дисциплины и выполнены практические и лабораторные задания

Оценка «хорошо» выставляется студенту, если достаточно полно изучен курс данной дисциплины и выполнены практические и лабораторные задания

Оценка «удовлетворительно» выставляется студенту, недостаточно если полно изучен курс данной дисциплины и выполнены практические и лабораторные задания

Оценка «неудовлетворительно» выставляется студенту, если отсутствуют знания и практические навыки по данной дисциплине

Оценка зачтено ставится студенту, если он в полном объеме выполнил практические и лабораторные задания, индивидуальные задания по предмету не менее, чем на 60%.

Оценка не зачтено ставится студенту, если он в неполном объеме выполнил практические и лабораторные задания или индивидуальные задания по предмету менее, чем на 60%.

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**

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

Процедура проведения данного оценочного мероприятия включает в себя: регулярный устный опрос в течение семестра по заранее заданным темам.

Предлагаемые студенту задания позволяют проверить следующие компетенции:

ОПК-3 .

Базовый уровень включает в себя умение устанавливать, настраивать и применять специализированное программное обеспечение для защиты информационных систем от внешних и внутренних атак в соответствии с требованиями ГОСТ и решать типовые профессиональные отвечать на вопросы базового уровня.

Повышенный уровень включает в себя умение использовать дополнительные настройки для защиты информации, осуществлять шифрование данных, настраивать параметры авторизации пользователей ПО, умение решать профессиональные задачи повышенной сложности и отвечать на вопросы повышенного уровня.

При подготовке к ответу студенту предоставляется право пользования конспектом лекций.

При проверке задания оцениваются, насколько хорошо студент ориентируется в изучаемой теме.

Составитель _____ А.С.Ермаков
(подпись)

«____»_____20 г.