СОЧИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)
федерального государственного автономного образовательного учреждения высшего образования
«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ»

Отделение среднего профессионального образования

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

"Безопасность функционирования информационных систем"

(наименование дисциплины)

Оценочные материалы рекомендованы МССН для специальности/профессии:

09.02.06 Сетевое и системное администрирование

(код и наименование специальности/профессии ОП СПО)

Освоение дисциплины ведется в рамках реализации основной образовательной программы среднего профессионального образования (ОП СПО):

"Сетевое и системное администрирование"

(наименование специальности/профессии ОП СПО)

Семестр реализации: 4 курс, 8 семестр

Сочи, 2021

1. НАЗНАЧЕНИЕ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

ФОС создается в соответствии с требованиями Федерального государственного образовательного стандарта для аттестации обучающихся на соответствие их достижений поэтапным требованиям соответствующей образовательной программы для проведения текущего оценивания, а также промежуточной аттестации обучающихся. ФОС является составной частью нормативно-методического обеспечения системы оценки качества освоения образовательной программы, входит в состав образовательной программы.

ФОС – комплект методических материалов, нормирующих процедуры оценивания результатов обучения, т.е. установления соответствия учебных достижений (результатов обучения) запланированным результатам освоения рабочих программ учебных дисциплин (модулей) и образовательных программ.

ФОС сформирован на основе ключевых принципов оценивания:

– валидности: объекты оценки должны соответствовать поставленным целям обучения;

– надежности: использование единообразных стандартов и критериев для оценивания достижений;

– объективности: разные обучающиеся должны иметь равные возможности добиться успеха.

ФОС подлежат ежегодному пересмотру и обновлению.

2. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Перечень контролируемых компетенций

Шифр	Компетенция
ПК 3.5.	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.
ПК 3.6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.
ПК 3.3.	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.
ПК 3.2.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
ПК 3.1.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.

3. ТЕКУЩИЙ КОНТРОЛЬ

3.1. Текущий контроль

Текущий контроль знаний используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной) обучающихся. Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы. Данный вид контроля стимулирует у обучающихся стремление к систематической самостоятельной работе по изучению дисциплины.

Оценочные средства позволяют провести текущий контроль по дисциплине. По каждому средству оценивается полнота и глубина освоения, характеризующиеся показателями и критериями оценивания

Показатель	Критерий	Шкала		
Пороговый (узнавание) «3»	Знает: базовые общие знания; Умеет: основные умения, требуемые для выполнения простых задач; Владеет: работает при прямом наблюдении.	3	2	1
Базовый (воспроизведение) «4»	Знает: факты, принципы, процессы, общие понятия в пределах области исследования; Умеет: диапазон практических умений, требуемых для решения определенных проблем в области исследования; Владеет: берет ответственность за завершение задач в исследовании, приспосабливает свое	4	3	2
Высокий (компетентность) «5» max балл	Знает: фактическое и теоретическое знание в пределах области исследования с пониманием границ применимости; Умеет: диапазон практических умений, требуемых для развития творческих решений, абстрагирования проблем; Владеет: контролирует работу, проводит оценку,	5	4	3

Максимальное количество баллов по каждому оценочному средству (соответствует вербальному критерию «высокий») представлено в Паспорте фонда оценочных средств и зависит от сложности темы и количества часов на ее усвоение.

3.2. Описание фонда оценочных средств

3.2.1. Критерии оценивания письменных и устных ответов обучающихся

С целью контроля и подготовки обучающихся к изучению новой темы может проводится устный опрос по предыдущим темам.
Критерии оценки:
– правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе);
– полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);
– осознанность ответа (учитывается понимание излагаемого материала);
– логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);
– рациональность использованных приемов и способов решения поставленной учебной задачи (учитывается умение использовать наиболее прогрессивные и эффективные способы достижения цели);
– своевременность и эффективность использования наглядных пособий и технических средств при ответе (учитывается способность грамотно и с пользой применять наглядность и демонстрационный опыт при устном ответе);
– использование дополнительного материала;
– рациональность использования времени, отведенного на задание (не одобряется затянутость устного ответа во времени, с учетом индивидуальных особенностей обучающихся).

Оценка «отлично» выставляется, если обучающийся: полно и аргументировано отвечает по содержанию задания; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; излагает материал последовательно и правильно.
Оценка «хорошо» выставляется, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
Оценка «удовлетворительно» выставляется, если обучающийся обнаруживает знание и понимание основных положений данного задания, но: излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки.
Оценка «неудовлетворительно» выставляется, если обучающийся обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «неудовлетворительно» отмечает такие недостатки в подготовке обучающегося, которые являются серьезным препятствием к успешному овладению последующим материалом.

3.2.2. Примерный перечень оценочных средств

3.2.3. Примеры оценочных средств

Примеры оценочных средств (при наличии) представлены в Приложении к рабочей программе дисциплины "Безопасность функционирования информационных систем"
Открыть приложение

3.3. Темы докладов, рефератов, презентаций

не предусмотренно

4. ПРОМЕЖУТОЧНЫЙ КОНТРОЛЬ

4.1. Оценочные средства для промежуточной аттестации

ФОС для промежуточной аттестации обучающихся по учебной дисциплине (модулю) Безопасность функционирования информационных систем предназначен для оценки степени достижения запланированных результатов обучения по завершению изучения дисциплины в установленной учебным планом форме и позволяют определить результаты

освоения дисциплины.
Рабочей программой предусмотрены:
- рубежный контроль по окончании изучения отдельных разделов программы;
- промежуточный контроль.
Формой контроля сформированности компетенций у обучающихся по учебной дисциплине (модулю) является:

Курс	Семестр	Вид контроля
4	8	Зачет с оценкой

4.2. Критерии оценивания

При оценке устного ответа учитываются: полнота и правильность ответа; степень осознанности, понимания изученного; языковое оформление ответа.

«5» ставится в том случае, если обучающийся: правильно понимает сущность вопроса, дает точное определение и истолкование основных понятий; строит ответ по собственному плану, сопровождает ответ новыми примерами, умеет применить знания в новой ситуации; может установить связь между изучаемым и ранее изученным материалом в том числе при изучении других предметов.

«4» ставится, если: ответ удовлетворяет основным требованиям к ответу на 5, но дан без использования собственного плана, новых примеров, применения знаний в новой ситуации, допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя.

«3» ставится, если обучающийся: правильно понимает сущность вопроса, но в ответе имеются отдельные пробелы в усвоении вопросов курса, не препятствующие дальнейшему усвоению программного материала; умеет применять полученные знания при решении простых задач по готовому алгоритму.

«2» ставится, если: обучающийся не овладел основными знаниями и умениями в соответствии с требованиями программы и допустил больше ошибок и недочетов, чем необходимо для оценки 3.

Оценка «1» ставится в том случае, если обучающийся не может ответить ни на один из поставленных вопросов.

Критерии оценки выполнения практического задания

Критерии оценки практического задания

«5» ставится если: обучающийся выполнил работу в полном объеме с соблюдением необходимой последовательности действий; получил правильные результаты и выводы; правильно и аккуратно выполнил все записи, вычисления, в рассуждениях и обосновании решения нет пробелов и ошибок; в решении нет математических ошибок (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).

«4» ставится, если работа выполнена полностью, но обоснования шагов решения недостаточны; выполнены требования к оценке 5, но допущены 2-3 недочета, или не более одной ошибки и одного недочета.

«3» ставится, если работа выполнена не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы; допущены более одной ошибки или более двух-трёх недочётов в выкладках, но учащийся владеет обязательными умениями по проверяемой теме.

«2» ставится, если работа выполнена не полностью и объем выполненной работы не позволяет сделать правильных выводов; работа проводилась неправильно, допущены существенные ошибки, показавшие, что обучающийся не владеет обязательные умениями по данной теме в полной мере.

«1» ставится, если: работа показала полное отсутствие у учащегося обязательных знаний и умений по проверяемой теме или значительная часть работы выполнена не самостоятельно.

Оценка «5» соответствует высокому уровню, оценка «4» – базовому, оценка «3» – пороговому.

4.3. Вопросы для промежуточной аттестации

1. Понятие информационной безопасности
2. Важность и сложность проблемы информационной безопасности
3. Основные составляющие информационной безопасности
4. Категории информационной безопасности
5. Основные определения и критерии классификации угроз
6. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
7. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна
8. Правовые средства защиты
9. Причины, виды и каналы утечки информации.
10. Классификация криптоалгоритмов
11. Симметричные криптосистемы
12. Асимметричные криптосистемы.
13. Обзор и классификация методов шифрования информации
14. Цифровая подпись
15. Аутенфикация и индефикация
16. Протоколы аутентификации
17. Биометрическая аутенфикация
18. Компьютерные вирусы
19. Структура и классификация компьютерных вирусов
20. Механизмы вирусной атаки
21. Антивирусные программы
22. Профилактические мероприятия для защиты компьютерных сетей от вредоносного ПО
23. Защита данных в автономном компьютере.
24. ПО и информационная безопасность
25. Резервное копирование
26. Проблема защиты электронной информации.
27. Место программно-математических методов в комплексной системе защиты информации.
28. Классификация угроз безопасности информации и возможные методы зашиты.
29. Резервное копирование данных: суть, устройства для хранения копии, рекомендации по резервному копированию.
30. Общий обзор программного обеспечения для профилактического обслуживания носителей информации и восстановления данных.
31. Эффектные меры, повышающие шансы восстановления информации на магнитных носителях.
32. Защита локального компьютера паролем включения: суть, алгоритм настройки, способы преодоления защиты.
33. Загрузка локального компьютера с использованием оригинальной дискеты: суть, программный пример, способы преодоления защиты.
34. Защита локального компьютера паролем заставки экрана, суть, алгоритм настройки, способы преодоления защиты.
35. Защита информации скрытием файлов и папок, изменением имени и расширения, атрибутом «только для чтения»: алгоритмы настройки, способы преодоления защиты.
36. MS Office: алгоритмы защиты документов от несанкционированного доступа и использования. Правила задания пароля. Способы преодоления защиты.
37. Особенности строения файлов текстовых процессоров. Алгоритмы уничтожения удалённого и исправленного текста в теле файла текстового процессора.
38. Применение программ-архиваторов для скрытия и защиты файлов. Правила задания пароля. Способы преодоления защиты.
39. Генератор паролей, алгоритмы генерации. Оценка стойкости пароля.
40. Временные файлы, причины появления временных файлов. Удаление временных

файлов программными методами и вкруговую.
41. Программное обеспечение для полного уничтожения удалённых файлов. Алгоритмы работы программ.
42. Алгоритмы настройки защиты дисков, папок, файлов в локальной сети. ПО для защиты компьютера от проникновения из внешней среды. Суть работы программ....
43. Электронная почта: алгоритм отправки сообщении, возможность перехвата, способы защиты. Отправка анонимных сообщении.
44. Опасность программ-апплетов Java, JavaScript. ActiveX. Алгоритмы настроим защиты браузеров. Опасность файлов «cookie». Методы контроле записи файлов «cookie» на жесткий диск.
45. Принцип работы прокси-сервера. Безопасные узлы. алгоритмы проверки безопасности.
46. Классификация компьютерных вирусов с позиции программно-математических методов, краткая характеристика каждого вида. Общие признаки заражения. Файловые вирусы: краткая характеристика перезаписывающего и паразитного вирусов
47. Файловые вирусы: наиболее общий алгоритм работы, алгоритм обнаружения вирусов, возможность восстановления файлов.
48. Загрузочный вирус, алгоритм получения управления вирусом. Алгоритмы предотвращения заражения, обнаружения заражения, удаления вируса.
49. Макровирусы, принципы устройства и функционирования. Алгоритмы обнаружения вирусов и обезвреживания файлов.
50. Вирусы, передающиеся по сети (сетевые, HTML-вирусы, вирусы-апплеты, троянские кони) и способы защиты от них.
51. Резидентные вирусы: краткая характеристика алгоритмов работы.
52. Резидентные вирусы, обнаружение и обезвреживание, возможность восстановления файлов.
53. Последовательность действий при обнаружении заражения вирусом. Правила предотвращения заражения вирусом

4.4. Перечень компетенций, которые сформированы у обучающихся при успешном выполнении заданий

В результате изучения учебной дисциплины обучающиеся осваивают следующие компетенции:

Раздел/Тема	Компетенции
Администрирование сетевых служб.	ПК 3.5., ПК 3.6., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1.
Безопасное администрирование сетевых служб в LINUX	ПК 3.5., ПК 3.6., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1.
Внедрение инфраструктуры открытых ключей	ПК 3.5., ПК 3.6., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1.
Внедрение, конфигурирование и обеспечение безопасности службы каталога Active Directory для Windows Server.	ПК 3.5., ПК 3.6., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1.
Обеспечение работоспособности и доступности серверов	ПК 3.5., ПК 3.6., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1.
Основы проектирования и эксплуатации защищенных информационных систем	ПК 3.5., ПК 3.6., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1.

5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, ПРАКТИЧЕСКОГО ОПЫТА, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Изучение дисциплины Безопасность функционирования информационных систем является базой для освоения студентами курсов профессионального цикла, формирует базу для овладения профессиональными компетенциями, которые могут быть применены в видах профессиональной деятельности в соответствии с Государственным образовательным стандартом профессионального образования.

В процессе изучения дисциплины предполагается проведение практических занятий для закрепления теоретических знаний, тематика практических занятий учитывает специфику получаемой специальности.

С целью закрепления и систематизации знаний, формирования самостоятельного мышления в программе предусмотрены часы для самостоятельной работы студентов.

При изучении дисциплины - внимание студента будет обращено на её прикладной характер, на то, где и когда изучаемые теоретические положения и практические навыки могут быть использованы в будущей практической деятельности.