Утверждаю

Зам. директора по УР

«31» 08 2022 г.

Иванешко И.В.

Согласовано

Системный администратор

ООО «Элком -Электро»

«31» 08 2022 г.

Ю. В. Скряго

Контрольно-оценочные материалы для промежуточной аттестации по междисциплинарному курсу МДК 03.02 Безопасность компьютерных сетей для специальности 09.02.06 Сетевое и системное администрирование

Дифференцированный зачет является промежуточной формой контроля, подводит итог освоения МДК 03.02 Безопасность компьютерных сетей

Профессиональные компетенции:

Код	*Профессиональных компетенций*
ПК 3.1	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
ПК 3.2	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
ПК 3.3.	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.
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.

Общие компетенции:

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 9.	Использовать информационные технологии в профессиональной деятельности

Дифференцированный зачет по МДК 03.02. Безопасность компьютерных сетей проводится в форме тестирования.

Тест содержит 20 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блоков (состоящих первый блок 50 вопросов, второй блок 60 вопросов) заданий по 10 вопросов. Время тестирования – 90 минут для каждой подгруппы (по 3 минуты на каждый вопрос из первого блока, по 6 минут на каждый вопрос закрытого типа).

Критерии оценивания

«5 баллов » - получают студенты, справившиеся с работой 100-90%;
«4 балла » - ставится в том случае, если верные ответы составляют 89-76% от общего количества;
«3 балла » - соответствует работа, содержащая 60-75% правильных ответов;
«2 балла» - соответствует работа, содержащая менее 60% правильных ответов.

Шкала оценивания образовательных результатов:

Оценка	Критерии
5 «отлично»	Студент набрал 5 баллов
4 «хорошо»	Студент набрал 4 балла
3 «удовлетворительно»	Студент набрал 3 балла
2 «неудовлетворительно»	Студент набрал 0-2 балла

Первый блок
Формируемые компетенции ПК.3.1, ПК 3.3, ПК 3.6, ОК01, ОК02, ОК09

1. Что такое фишинг?
a) Техника безопасности, используемая для защиты сетевых ресурсов.
b) Незаконные действия для получения личной информации пользователей.
c) Программа для выявления компьютерных вирусов.
2. Какую роль играет пароль в кибербезопасности?
a) Защищает от вирусов и вредоносных программ.
b) Позволяет пользователям получать доступ к защищенным ресурсам.
c) Обеспечивает шифрование информации.
3. Что такое двухфакторная аутентификация?
a) Метод защиты, использующий два разных пароля.
b) Метод проверки личности, который требует двух независимых подтверждений.
c) Метод защиты, использующий шифрование данных.
4. Что такое межсетевой экран (firewall)?
a) Программа для защиты от вредоносных программ.
b) Оборудование или программное обеспечение, контролирующее потоки данных между сетями.
c) Технология шифрования информации.
5. Что такое DDoS-атака?
a) Попытка получить несанкционированный доступ к системе.
b) Атака на сервер, ограничивающая его доступность.
c) Защитная система, предотвращающая атаки на сеть.
6. Что такое сетевая угроза "мальварь" (malware)?
a) Приложение, разработанное для защиты данных пользователя.
b) Вредоносное программное обеспечение, созданное с целью нанесения вреда системе или укравшие данные пользователя.
c) Слово, применяемое для описания сигналов или шума в сетях передачи данных.
7. Что такое "фаерфокс" (Firefox)?
a) Один из наиболее популярных интернет-браузеров.
b) Протокол безопасной передачи данных.
c) Система защиты, используемая в криптографии.
8. Что такое "пинг" (ping)?
a) Программа для проверки доступности сетевых узлов.
b) Сетевая угроза, направленная на взлом платежных систем.
c) Метод шифрования информации.
9. Что такое "фильтр спама" (spamfilter)?
a) Программа или устройство, фильтрующее нежелательные электронные сообщения.
b) Шифрование данных для их защиты от несанкционированного доступа.

c) Комплексная система защиты информации в сети.
10. Что такое "вирус" в контексте компьютерной безопасности?
a) Программа для проверки системы на наличие уязвимостей.
b) Программа, распространяющаяся и внедряющаяся в систему без разрешения пользователя, вызывая различные проблемы.
c) Система, обеспечивающая шифрование данных и их безопасность.
11. Очень сложные пароли гарантируют 100% защиту?
А.Нет
Б.Да, если после работы полностью очищать куки и не хранить пароль на компьютере
В.Да, если пароль не сохранен на компьютере
12.Какие вирусы активизируются после включения ОС?
А.Снифферы
Б.Загрузочные
В.Трояны
Г.Черви
13.Представляют ли угрозу вирусы для крупных компаний?
А.Нет
Б.Да, представляют
В.Скорее нет. В крупных компаниях развита система безопасности
Г.Если компания обладает сотрудниками занимающимися безопасностью сети, вирусы не могут нанести такому предприятию вреда
14.С чем связана атака введением произвольных запросов в базу данных?
А.Уязвимость SQL Injection
Б.Сбой Denial of Service
В.Ошибка Denial of Service
Г.Неполадка PHP Include
15.Фильтрация контента, для чего она служит?
А.Защищает от скрытой загрузки вредоносного программного обеспечения
Б.Помогает быстро находить в сети требуемый контент сохраняя при этом много драгоценного времени
В.Отключает назойливую рекламу
Г.Отсеивает поисковый спам
16.Какой уровень безопасности трафика обеспечивает WPA2?
А.Высокий
Б.Низкий
В.Достаточный для домашней сети
Г.Средний
17.Сколько минимально символов должен содержать безопасный пароль, состоящий из латинских строчных букв?
А.15
Б.8
В.10
Г.6
18.Какую угрозу можно назвать преднамеренной? Сотрудник:
А.Открыл письмо содержащее вредоносное ПО
Б.Ввел неправильные данные
В.Совершил не авторизованный доступ
Г.Включил компьютер без разрешения
19. Безопасно ли вводить пароли простым копированием?
А.Безопасно если это мой компьютер
Б.Да
В.Безопасно если после работы очистить куки

Г.Нет
20.Какую защиту необходимо использовать против программы iris или ее аналогов?
А.Шифровать трафик
Б.Использовать очень сложные пароли
В.Устанавливать только лицензионные антивирусы
Г.Не пользоваться Wi-fi
21. Что может привести к заражению компьютера?
А.Получение сообщения по электронной почте
Б.Загрузка пиратского ПО
В.Создание нового файла
Г.Отправка сообщения по электронной почте
22. Что такое Brute Force?
А.Взлом методом заражения системы через вредоносный файл
Б.Метод заставляющий пользователя самому раскрыть конфиденциальную информацию
В.Получение конфиденциальной информации с компьютера методом электронной рассылки
Г.Взлом методом перебора паролей
23. В каком блок файле autorun.inf чаще всего прописывается вредоносная программа?
А.Open
Б.Setup
В.Downloade
Г.Dll
24Как называется преднамеренно внесенный в программное обеспечение объект, приводящий к действиям программного обеспечения не предусмотренным производителем, приводящим к нарушению конфиденциальности и целостности информации?
А.Троян
Б.Бэкдор
В.Закладка
Г.Вирус
25Безопасно ли сохранять пароли в автозаполнении браузера?
А.Да, если пароль к входу в систему знаю только я один
Б.Нет
В.Да, если этим компьютером пользуюсь только я один
Г.Да
26. Для чего служит DLP? Система выполняет функцию:
А.Защита компьютера от вирусов
Б.Выполняет функцию безопасного ввода паролей
В.Предотвращает утечку информации с компьютера
Г.Предупреждает пользователя о попытках взлома и хакерских атаках
27. Антивирус полностью защищает компьютер от вирусов и атак при работе в сети. Вы согласны с этим?
А.Нет
Б.Да, если это лицензионный антивирус известного производителя
В.Защищает совместно с включенным бродмауэром
Г.Да
28. Самый лучший способ хранения паролей в информационной системе?
А.Хеширование
Б.Вообще не сохранять
В.Архивирование
Г.Хранить только с включенным брандмауэром
29. Какое минимальное количество символов должен содержать пароль входа субъектов в систему АС, при классе защищенности 1А?
А.12

Б.8
В.10
Г.15
30. На каких системах более динамично распространяются вирусы?
AL.inux
Б.MacOS
В.Android
Г.Windows

Формируемые компетенции
ПК3.2, ПК 3.4 ПК 3.6, , ОК01, ОК02, ОК09

31. Самая массовая угроза компьютерной безопасности, это:
А.Спам
Б.Трояны
В.Черви
Г.Шпионские программы
32. Если компьютер работает в нормальном режиме, означает ли это что он не заражен?
А.Нет
Б.Если не изменилась скорость работы, компьютер совершенно чист
В.Да
Г.Если антивирус ничего не показывает компьютер чист
33. Установка одновременно нескольких антивирусных программ повышает защищенность. Вы согласны с этим?
А.Да
Б.Да, если это антивирусы от известных производителей
В.Да, если это антивирусы одного производителя
Г.Нет
34. Что чаше всего используют злоумышленники при атаке на компьютеры должностных лиц и руководителей крупных компаний?
А.Фишинг
Б.Спам
В.Загрузка скрытого вредоносного ПО
Г.DDos атаки
35. Как гарантировать 100% защищенность компьютера от заражения вирусами в сети?
А.Включить брандмауэр
Б.Установить новое программное обеспечение
В.Таких гарантий нет
Г.Посещать только сайты известных брендов
36. Что необходимо выполнять для контроля безопасности электронной почты?
А.Часто сменять пароли
Б.Проверять страницу посещения
В.Регистрировать почтовый ящик только в известных системах
Г.Использовать сложные пароли
37. Что такое Firewall, для чего он нужен?
А.для фильтрации трафика
Б.для очистки компьютера
В.для быстрого и безопасного поиска информации
Г.для форматирования
38. Обеспечивает ли форматирование жесткого диска полное избавление от вирусов?
А.Обеспечивает полностью
Б.Обеспечивает если выполнено быстрое форматирование
В.Нет

Г.Обеспечивает при низкоуровневом форматировании
39. Можно ли хранить важную информацию на жестком диске компьютера, в том числе пароли?
А.Да, если это мой личный компьютер
Б.Да
В.Нет
Г.Да, если компьютер не подключен к интернету
40. Если не нажимая на иконки просто просмотреть подозрительный сайт, ничего не произойдет. Вы согласны?
А.Нет. Заражение может произойти даже если вы просто посмотрели информацию с экрана, при этом ничего не нажимая
Б.Да, простой просмотр не наносит никакого вреда
В.Да, заражение происходит только после кликов, чем запускается вирусная программа
41. Что может привести к заражению компьютера?
А.Получение сообщения по электронной почте
Б.Загрузка пиратского ПО
В.Создание нового файла
Г.Отправка сообщения по электронной почте
42. Что такое Brute Force?
А.Взлом методом заражения системы через вредоносный файл
Б.Метод заставляющий пользователя самому раскрыть конфиденциальную информацию
В.Получение конфиденциальной информации с компьютера методом электронной рассылки
Г.Взлом методом перебора паролей
43. В каком блок файле autorun.inf чаще всего прописывается вредоносная программа?
А.Open
Б.Setup
В.Downloade
Г.Dll
44Как называется преднамеренно внесенный в программное обеспечение объект, приводящий к действиям программного обеспечения не предусмотренным производителем, приводящим к нарушению конфиденциальности и целостности информации?
А.Троян
Б.Бэкдор
В.Закладка
Г.Вирус
45Безопасно ли сохранять пароли в автозаполнении браузера?
А.Да, если пароль к входу в систему знаю только я один
Б.Нет
В.Да, если этим компьютером пользуюсь только я один
Г.Да
46. Для чего служит DLP? Система выполняет функцию:
А.Защита компьютера от вирусов
Б.Выполняет функцию безопасного ввода паролей
В.Предотвращает утечку информации с компьютера
Г.Предупреждает пользователя о попытках взлома и хакерских атаках
47. Антивирус полностью защищает компьютер от вирусов и атак при работе в сети. Вы согласны с этим?
А.Нет
Б.Да, если это лицензионный антивирус известного производителя
В.Защищает совместно с включенным бродмауэром
Г.Да
48. Самый лучший способ хранения паролей в информационной системе?

А.Хеширование
Б.Вообще не сохранять
В.Архивирование
Г.Хранить только с включенным брандмауэром
49. Какое минимальное количество символов должен содержать пароль входа субъектов в систему АС, при классе защищенности 1А?
А.12
Б.8
В.10
Г.15
50. На каких системах более динамично распространяются вирусы?
AL.inux
Б.MacOS
В.Android
Г.Windows

Второй блок

Формируемые компетенции
ПК 3.1, ПК 3.2, ПК 3. , ОК01, ОК02, ОК09

1.Что такое межсетевой экран?
2. Каковы преимущества частных сетей?
3.Какое высказывание наиболее точно характеризует шифрование?
4. Почему NIDS называется так?
5. Где в системе Solaris располагаются файлы загрузки?
6. Что относится к основными средствами управления AD?
7. Что позволяет порт 80?
8. Какая служба безопасности является наиболее критичной для электронной коммерции?
9.Что является основной причиной распространения использования беспроводных технологий?
10.Что относится к основным категориям атак?
11. Что относится к основным видам мотивации хакеров?
12.Какие службы безопасности предназначаются для защиты от атак доступа?
13.Какие ключевые этапы включаются в процесс обеспечения информационной безопасности?
14. Аутентификация личности в компьютерных системах может быть реализована при помощи чего?
15. Сколько интерфейсов у межсетевого экрана прикладного уровня?
16.Какие аспекты безопасности обеспечиваются при помощи шифрования в целом?
17.Сколько существует основных типов датчиков HIDS?
18.Какие сервисы обычно запускаются при помощи файлов загрузки?
19.Для выполнения каких действий могут использоваться групповые политики (GP)?
20. В каком файле должны быть определены файлы .cgi и .pl, чтобы программы выполнялись без отображения исходного кода на веб-странице?
21.Радиус действия обычной беспроводной системы стандарта 802.11x в помещениях составляет, как правило сколько меторов?
22. Что такое атака доступа?
23. Для защиты от атак какого типа предназначена служба конфиденциальности?
24.Что входит в величину ущерба, нанесенного при совершении компьютерного преступления?
25.Какие разделы политики являются общепринятыми?
26. Что такое уязвимость?

27. В какой последовательности должны проходить процессы обеспечения информационной безопасности и управление риском?
28.Процедура управления пользователями что определяет?
29. Какая система получила сертификат уровня А1 "Оранжевой книги"?
30. Какой тип экранов более безопасен?

Формируемые компетенции
ПК 3.4, ПК 3.5, ПК 3.6, ОК01, ОК02, ОК09

31. В чем основное различие между типами VPN?
32.Какой файл используется для настройки запрещающей конфигурации TCP-Wrappers?
33. К основным возможностям утилиты secedit.exe относится?
34.Какое назначение службы DNS?
35.Какие требования предъявляются к корневому каталогу веб-сервера?
36. Какой алгоритм используется WEP для обеспечения конфиденциальности?
37. Что такое атака модификации?
39.Какие политики и процедуры необходимо разработать после завершения шага оценки?
40.Какие системы будут защищены межсетевым экраном, если почтовый сервер компании разместить между маршрутизатором и экраном?
41.Что такое пользовательская VPN?
42.Какие события в системе рекомендуется фиксировать в большинстве случаев?
43.Какое подключение к провайдеру является наиболее надежным?
44.Какие основные меры необходимо предпринять для защиты сервера от атак злоумышленника через интернет?
45.Какой алгоритм используется WEP для обеспечения целостности?
46.Какую из возможных угроз для безопасности системы труднее всего обнаружить?
47.Какую службу можно описать следующим образом: "обеспечивает секретность информации, открывает доступ к информации только аутентифицированным пользователям?"
48.К каким организациям применяются правила закона HIPAA?
49.Какие виды доступа к файлам имеются?
50.Какие знания необходимы агентам угроз для нанесения ущерба?
51.Когда сотрудники организации должны в первый раз проходить обучение безопасности?
52.Какие параметры могут использоваться в биометрических системах?
53.Какие системы будут защищены межсетевым экраном, если почтовый сервер компании разместить за маршрутизатором и экраном?
54.Каковы преимущества пользовательских VPN?
55.Какими способами могут подвергнуться атакам системы шифрования?
56.Сколько сетевых карт обычно используется в NIDS?
57.В каком файле в ОС Solaris хранятся настройки требований к паролю?
58.Какие службы следует размещать в DMZ?
59.Какие порты следует разрешить для доступа к серверу электронной коммерции?
60. Какой из стандартов аутентификации в WLAN наиболее надежен?

Составил преподаватель Скряго О.С.