Утверждаю
Зам. директора по УР
«31» 08 2023г.
Иванешко И.В.

Согласовано
Ведущий специалист-эксперт отдела по защите информации ГУ-ОПФ по Смоленской области
«31» 08 2023г.
Ефремов А.А.,

Контрольно-оценочные средства для промежуточной аттестации

по учебной практике УП.02
для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Дифференцированный зачет является промежуточной формой контроля, подводит итог освоения учебной практики УП.02 .

Профессиональные компетенции:

ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

Общие компетенции:
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 09. Использовать информационные технологии в профессиональной деятельности.

Дифференцированный зачет по учебной практике УП.02 проводится в форме тестирования.

Тест содержит 10 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блоков (состоящих первый блок 50 вопросов, второй блок 50 вопросов) заданий по 5 вопросов. Время тестирования – 45 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
«отлично»	Студент набрал 5 баллов
«хорошо»	Студент набрал 4 балла
«удовлетворительно»	Студент набрал 3 балла
«неудовлетворительно»	Студент набрал 0-2 балла

Первый блок

Формируемые компетенции ОК 01, ОК2, ОК3, ОК9, ПК 2.1, 2.3

1. Для чего создан анонимный STP-сервер?

Варианты ответа:

а) создания ботнета

б) распределенных вычислений сложных математических задач

в) размещения на них сайтов с порнографической или другой запрещенной информацией

г) рассылки спама

2. Что такое метаморфизм?

Варианты ответа:

а) метод маскировки от антивирусов с помощью многоуровневого архивирования и запаковки

б) метод маскировки от антивирусов с помощью шифрования

в) создание вирусных копий путем шифрования части кода и/или вставки в код файла дополнительных, ничего не делающих команд

г) создание вирусных копий путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, ничего не делающих команд

3. Какие свойства должны быть обязательные для любого современного антивирусного комплекса?

Варианты ответа:

а) быть кроссплатформенным (работать под управлением любой операционной систем

б) не мешать выполнению основных функций компьютера +

в) интегрироваться в браузер

г) не занимать много системных ресурсов

д) не занимать канал Интернет

е) надежно защищать от вирусов

4. Что за задача, выполняющая модуль планирования, входящий в антивирусный комплекс?

Варианты ответа:

а) определения параметров взаимодействия различных компонентов антивирусного комплекса

б) настройки параметров уведомления пользователя о важных событиях в жизни антивирусного комплекса

в) настройка расписания запуска ряда важных задач (проверки на вирусы, обновления антивирусных баз и пр.)

г) определения областей работы различных задач поиска вирусов

5. К каким методам антивирусной защиты относит использование брандмауэров?

Варианты ответа:

а) техническим

б) теоретическим

в) практическим

г) организационным

6. Каковы вы преимущества сигнатурного метода антивирусной проверки над эвристическим?

Варианты ответа:

а) существенно менее требователен к ресурсам

б) не требует регулярного обновления антивирусных баз

в) позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

г) более надежный

7. Антивирусные базы можно обновить на компьютере, не подключенном к Интернет?

Варианты ответа:

а) нет

б) да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы

в) да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором

8. Какова основная задача, которую решает антивирусная проверка в режиме реального времени?

Варианты ответа:

а) обеспечение невмешательства в процесс деятельности других программ

б) предоставление возможности глубокой проверки заданных объектов

в) обеспечение взаимодействия между пользователем и антивирусной программой

г) обеспечение непрерывности антивирусной проверки

9. Чем может быть вызвана подозрительная сетевая активность может?

Варианты ответа:

а) логической бомбой

б) сетевым червем

в) трояном

г) P2P-червем

10. Что такое RAID-массив?

а) Набор жестких дисков, подключенных особым образом;

б) Антивирусная программа;

в) Вид хакерской утилиты;

г) База защищенных данных;

д) Брандмауэр.

11. Какие есть методы реализации антивирусной защиты?

а) аппаратные и программные;

б) программные, аппаратные и организационные

в) только программные

г) достаточно резервного копирования данных.

12. Что входит в ячейку резервного копирования и восстановления HP Data Protector? (Выберите несколько правильных ответов)

Варианты ответа:

а) сервер управления Cell Manager

б) различное офисное оборудование: принтеры, факсы и пр.

в) устройства хранения резервных копий

г) клиентские серверы, рабочие станции, ноутбуки и пр.

д) коммутационное оборудование: свитчи, хабы, роутеры и пр.

13.Перечислите элементы ячейки резервного копирования и восстановления HP Data Protector?

Варианты ответа:

а) принтеры и факсы

б) серверы установки Installation Server

в) телефоны и телефонные станции

г) клиентские серверы, рабочие станции, ноутбуки и пр.

д) устройства хранения резервных копий

14. Выделите основные компоненты ячейки резервного копирования и восстановления HP Data Protector?

Варианты ответа:

а) сетевая инфраструктура

б) сервер управления Cell Manager

в) коммутационное оборудование: свитчи, хабы, роутеры и пр.

г) устройства хранения резервных копий

15. Что входит в список требований при выборе сервера резервного копирования и восстановления HP Data Protector?

Варианты ответа:

а) поддержка платформы сервера: тип ОС, процессора
б) наличие хорошей видео-карты на сервере
в) наличие прав Администратора на сервере
г) к серверу должен быть подключен принтер
д) проверить свободен ли порт 5555
16. Какие требования при выборе сервера резервного копирования и восстановления HP Data Protector?
Варианты ответа:
а) к серверу должен обязательно быть подключен ленточный драйв
б) оценить надежность сервера
в) установлена как минимум Windows 2012
г) поддерживаемый браузер на сервере
д) установлен и работает ли протокол TCP/IP
17. Каковы основные требования при выборе сервера резервного копирования и восстановления HP Data Protector?
Варианты ответа:
а) проверка не занятости сетевых портов
б) подойдет абсолютно любой сервер, даже старый
в) оценить рост внутренней базы данных
г) поддержка версии Windows и ее релиза
18. Из каких шагов состоит установка HP Data Protector?
Варианты ответа:
а) Выбрать каталог установки программного продукта
б) выбрать тип установки: сервер, клиент, GUI
в) задать служебного пользователя для запуска служб
г) указать устанавливать ли модуль автоматического обновления
д) задать адрес сервера установки
19. Какие есть шаги по установке HP Data Protector?
Варианты ответа:
а) задать номер служебного порта для служб
б) установить дополнительные компоненты в отдельную папку на сервере
в) выбрать из списка дополнительные компоненты
г) выбрать тип установки: сервер, клиент, GUI
д) указать каталог установки программного продукта
20. Каковы шаги по установке HP Data Protector?
Варианты ответа:
а) задать служебного пользователя для запуска служб
б) задать адрес сервера установки
в) задать номер служебного порта для служб
г) выбрать каталог установки программного продукта
д) установить все нужные компоненты
21. Какие есть элементы, входящие в выпадающий список поля выбора контекста в графическом интерфейсе HP Data Protector?
Варианты ответа:
а) мониторинг (Monitor)
б) ошибки (Errors)
в) восстановление (Restore)
г) пользователи (Users)
д) логи (Logs)

22. Какие есть элементы, входящие в выпадающий список поля выбора контекста в графическом интерфейсе HP Data Protector?
Варианты ответа:
а) серверы (Servers)
б) клиенты (Clients)

в) устройства и носители (Devices & Media)
г) резервирование (Backup)
д) ошибки (Errors)
23. Каковы элементы, входящие в выпадающий список поля выбора контекста в графическом интерфейсе HP Data Protector?
Варианты ответа:
а) операции с объектами (Object Operations)
б) логи (Logs)
в) ошибки (Errors)
г) внутренняя база (Internal Database)
д) отчеты (Reporting)
24. Какие еще дополнительные возможности по резервному копированию и восстановлению присутствуют в HP Data Protector?
Варианты ответа:
а) создание отказоустойчивой системной копии (Disaster Recovery)
б) снижение объемов хранения полных копий на дисковых носителях (Virtual Full Backup)
в) поддержка механизма быстрых дисков SSD (Fast Disk Access)
г) безостановочное резервное копирование данных приложения (Online Backup)
25. Какие есть дополнительные возможности по резервному копированию и восстановлению с помощью HP Data Protector?
Варианты ответа:
а) поддержка беспроводных сетей (Wi-Fi Network Access)
б) снижение объемов хранения резервных копий (Дедупликация)
в) поддержка технологий мгновенных снимков при резервном копировании (Zero Downtime Backup)
г) общедоступный интерфейс разработчика (Common Program Interface)
д) поддержка технологий мгновенных снимков при восстановлении (Instant Recovery)

Формируемые компетенции ОК 01, ОК2, ОК3, ОК9, ПК 2.2

26. Администрирование межсетевого экрана как должно всегда выполняться? (Выберите несколько правильных ответов)
Варианты ответа:
а) По защищенному каналу.
б) Из интернета – по защищенному каналу и с использованием строгой аутентификации.
в) Из локальной сети возможно администрирование без выполнения строгой аутентификации.
г) С использованием строгой аутентификации.
27. Какие из перечисленных веб-серверов следует расположить во внешней DMZ? (Выберите несколько правильных ответов)
Варианты ответа:
а) Веб-сервер, на котором осуществляется on-line'овый заказ товаров.
б) Веб-сервер, на котором публикуются распоряжения руководства организации.
в) Веб-сервер, на котором могут находиться личные данных сотрудников.
г) Веб-сервер, на котором опубликованы общедоступные телефоны и координаты организации.
28. Какие из перечисленных серверов Вы расположили бы во внешней DMZ?
Варианты ответа:
а) Сервер базы данных.
б) Почтовый сервер.
в) Сервер с бухгалтерскими данными.
г) Аутентификационный сервер.
29. Какие из перечисленных DNS-серверов Вы расположили бы во внутренней DMZ? (Выберите несколько правильных ответов)
Варианты ответа:
а) DNS-сервер, содержащий записи о почтовом сервере.

б) DNS-сервер, содержащий записи о сервере базы данных.
в) DNS-сервер, содержащий записи о сервере с бухгалтерскими данными.
г) DNS-сервер, содержащий записи о веб-сервере с возможностями on-line'овых заказов.
30. Встроенный в ОС межсетевой экран по сравнению с аппаратным межсетевым экраном обеспечивает что?
Варианты ответа:
а) Лучшую защиту.
б) Лучшую масштабируемость.
в) Лучшую аутентификацию.
31. Какова предпочтительная последовательность этапов внедрения межсетевого экрана?
Варианты ответа:
а)
планирование
конфигурирование
тестирование
развертывание
управление
б)
конфигурирование
планирование
тестирование
развертывание
управление
в)
развертывание
планирование
тестирование
конфигурирование
управление
г)
планирование
конфигурирование
управление
развертывание
тестирование
32. Какой сетевой уровень, на котором функционируют коммутаторы?
Варианты ответа:
а) Первый уровень.
б) Второй уровень.
в) Третий уровень.
г) Седьмой уровень.
33. Что следует выполнить на этапе планирования внедрения межсетевого экрана? (Выберите несколько правильных ответов)
Варианты ответа:
а) Идентифицировать угрозы и уязвимости для каждой информационной системы.
б) Определить потенциальное воздействие и величину вреда, который может нанести потеря конфиденциальности, целостности или доступности информационных активов организации или предоставляемых ею сервисов.
в) Проанализировать возможности управления выбранным межсетевым экраном.
г) Проанализировать значения по умолчанию всех параметров.

34.При анализе назначения межсетевого экрана что следует определить? (Выберите несколько правильных ответов)
Варианты ответа:
а) Какие типы трафика должны защищаться.

б) Какие типы технологий межсетевых экранов лучше всего подходят для трафика, который должен быть защищен.
в) Какие дополнительные возможности безопасности – такие как возможности обнаружения проникновения, VPN, фильтрование содержимого – должен поддерживать межсетевой экран.
г) Какие способы управления поддерживает данный межсетевой экран.
35. При анализе возможностей управления межсетевым экраном, что следует определить?
Варианты ответа:
а) Какие протоколы должен поддерживать межсетевой экран для удаленного управления, например, HTTP-поверх-SSL, SSH или доступ по последовательному порту.
б) Могут ли быть отключены протоколы удаленного управления, если они не приемлемы для организации и не соответствуют ее организационной политике.
в) Может ли удаленное управление быть ограничено определенными интерфейсами на межсетевом экране и IP-адресами источника, например, принадлежащими конкретной внутренней сети.
г) Какой трафик должен защищаться.
37.При анализе возможностей управления межсетевым экраном, что следует определить?
(Выберите несколько правильных ответов)
Варианты ответа:
а) Какое количество портов существует на выбранном экземпляре межсетевого экрана.
б) Можно ли в интерфейсе межсетевого экрана группировать различные типы трафика в одном правиле.
в) Поддерживает ли межсетевой экран централизованное управление несколькими устройствами (не обязательно только межсетевыми экранами) от одного производителя.
г) Если централизованное управление возможно, выполняется ли оно специфичным для производителя приложением или может выполняться стандартными приложениями, например, через веб-интерфейс.
38. При анализе производительности межсетевого экрана, что следует определить? (Выберите несколько правильных ответов)
Варианты ответа:
а) Какую пропускную способность, максимальное количество одновременно открытых соединений, соединений в секунду может обеспечивать межсетевой экран.
б) Возможна ли балансировка нагрузки и резервирование для гарантирования высокой отказоустойчивости.
в) Что является более предпочтительным – аппаратный или программный межсетевой экран.
г) Какое количество портов существует на выбранном экземпляре межсетевого экрана.
39. Для анализа возможностей интеграции межсетевого экрана с сетевой инфраструктурой, что следует определить? (Выберите несколько правильных ответов)
Варианты ответа:
а) Требуется ли для межсетевого экрана специализированная аппаратура для корректной интеграции в сетевую инфраструктуру организации (специфические требования подключения к электричеству, специфический тип сетевого интерфейса (NIC), специфические устройства резервного копирования и т.п.).
б) Необходима ли для межсетевого экрана совместимость с другими устройствами в сети или сервисами, которые обеспечивают безопасность.
в) Существует ли интеропрерабельность логов, создаваемых межсетевым экраном, с существующими системами управления логами.
г) Потребует ли установка межсетевого экрана каких-либо изменений в других сегментах сети. +

40. При внедрении персональных межсетевых экранов и межсетевых экранов для хостов, что следует рассмотреть? (Выберите несколько правильных ответов)
Варианты ответа:
а) Удовлетворяют ли рабочие станции и сервера минимальным системным требованиям, которые необходимы для функционирования межсетевого экрана.

б) Будет ли межсетевой экран совместим с другим ПО обеспечения безопасности на рабочей станции или сервере (например, с ПО обнаружения вредоносного кода).
в) Возможно ли централизованное управление межсетевым экраном, и могут ли политики, которые обеспечивают безопасность организации, автоматически загружаться на клиентские машины. +
г) Необходимо ли изменить пароль администратора на рабочей станции.
41. Что следует рассмотреть при внедрении персональных межсетевых экранов и межсетевых экранов для хостов? (Выберите несколько правильных ответов)
Варианты ответа:
а) Могут ли отчеты о нарушениях с межсетевого экрана передаваться на центральный сервер.
б) Может ли блокироваться межсетевой экран кем-либо, кроме администратора, и может ли кто-либо изменить установки межсетевого экрана.
в) Будет ли межсетевой экран конфликтовать с персональным межсетевым экраном, встроенным в ОС. Если да, то как легко преодолеть этот конфликт.
г) Необходимо ли изменить пароль администратора на рабочей станции.
44.Тестирование межсетевого экрана должно включать какие шаги? (Выберите несколько правильных ответов)
Варианты ответа:
а) Пользователи могут устанавливать и поддерживать соединения через межсетевой экран.
б) Разрешенный трафик пропускается политикой, не разрешенный трафик блокируется.
в) Межсетевые экраны для хостов и персональные межсетевые экраны не препятствуют и не влияют на работу существующих приложений.
г) Обеспечивается адекватная производительность при нормальном и пиковом использовании.
45. Что включает в себя управление межсетевым экраном? (Выберите несколько правильных ответов)
Варианты ответа:
а) Сопровождение архитектуры, политик, ПО межсетевого экрана и других компонент, которые были развернуты. +
б) Обновление и последующее тестирование межсетевого экрана.
в) Изменение правил политик при обнаружении новых угроз и изменении требований, таких, например, как установка новых приложений или хостов.
г) Отслеживание производительности различных компонент межсетевого экрана.
46. На каком принципе основана защита компьютерных систем, предполагающая необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов?
Варианты ответа:
а) на принципе непрерывности защиты
б) на принципе системности защиты
в) на принципе гибкости защиты
г) на принципе разумной достаточности
47. каковы методы защиты от копирования информации?
Варианты ответа:
а) отключение принтера
б) удаление из компьютера накопителей для гибких CD-дисков
в) нестандартное форматирование носителя информации, перепрограммирование контроллеров внешнего запоминающего устройства, аппаратные регулировки и настройки, изменение алгоритма подсчета контрольной суммы
г) архивирование файлов
48. Какая технология используется для безопасной передачи данных по каналам интернет?
Варианты ответа:
а. Www
б. Dicom
в. Vpn
г. Ftp
д. Xml

49. Какова секретная информация, которая хранится вWindows? (Выберите несколько правильных ответов)
Варианты ответа:
а) пароли для доступа к сетевым ресурсам
б) пароли для доступа в Интернет
в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере+

50. На какие виды подразделяют криптосистемы? (Выберите несколько правильных ответов)
Варианты ответа:
а) симметричные
б) ассиметричные
в) с открытым ключом

Второй блок

Формируемые компетенции ОК1, ОК2, ОК3, ОК9, ПК2.1., ПК 2.3

1. Какие дополнительные возможности по резервному копированию и восстановлению, входящие в HP Data Protector Вы знаете?
2. Чем определяется система резервного копирования (СРК)?
3. На какие основные части делится регулярный процесс резервного копирования?
4. Какие точки сопряжения системы с платформой NAS Вы знаете?
5. Какая цель резервного копирования?
6. Какие задачи определяются из целей резервного копирования?
7. Как производится резервное копирование?
8. Резервное копирование БД производится не реже, какого времени?
9. Срок хранения резервной копии БД не менее, какого времени?
10. Что автоматически делает антивирусная программа в Microsoft Defender при установке и включении другого антивирусного приложения?
11. Что автоматически делает программа Microsoft Defender при удалении другого приложения?
12. Зеленый значок в антивирусной системе в отчете, что означает?
13. Красный значок в антивирусной системе в отчете, что означает?
14. Желтый значок в антивирусной системе в отчете, что означает?
15. Что означает автоматическое обновление программы и антивирусных баз?
16. Когда необходимо выполнять автоматическое сканирование?
17. Как может создаваться код аутентификации сообщения (MAC) может создаваться?
18. Атака «man in the middle» является чем?
19. Для чего используются в криптографии сдвиговые регистры с обратной связью?
20. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?
21. Какие сбои оборудования бывают?
22. Как расшифровывается аббревиатура DMZ?
23. Что должно располагаться в сети демилитаризованной зоны (DMZ)?
24. Что следует установить между DMZ и ISP?
25. Если в организации есть веб-сервер для внешних пользователей и веб-сервер для получения информации своими сотрудниками, то какого оптимальное количество DMZ?

Формируемые компетенции ОК1, ОК2, ОК3, ОК9, ПК2.2

26. Какие из сервисов реализуются при использовании криптографических преобразований?
27. Что позволяет предотвратить использование криптографических преобразовании
28. Перечислите механизмы защиты информационных систем от несанкционированного доступа.
29. Как называется атрибут беспроводной сети, позволяющий логически отличать сети друг от друга?
30. Что посылает устройство клиента во все радиоканалы в беспроводной локальной сети IEEE 802.11 в начале процесса открытой аутентификации?

31. Какой метод аутентификации стандарта IEEE 802.11 требует настройки статического ключа шифрования WEP, одинакового для точки доступа и клиентского устройства?

32. Что такое ICV в составе WEP-кадра?

33. На каком алгоритме шифрования основан CCMP (Counter-Mode with CBCMAC Protocol)?

34. На каком алгоритме шифрования основан WEP?

35. Какой механизм в составе WPA позволяет предотвратить перехват пакетов, содержание которых может быть изменено, а модифицированный пакет вновь передан по сети?

36. Для работы какого протокола необходимо, чтобы был сертифицирован только сервер аутентификации, а у клиентов сертификатов может не быть?

37. Для чего предназначены системы IDS?

38. Для какого типа сетевых систем обнаружения вторжений критично иметь надежную информацию о том, как ведет себя сеть в нормальных условиях – точку отсчета?

39. Какие точки сопряжения системы с платформой NAS Вы знаете?

40. Какие типы томов обеспечивают защиту от сбоев?

41. Какой тип тома обеспечивает максимальную производительность выполнения дисковых операций?

42. Какой тип диска требуется для создания отказоустойчивых томов?

43. С какой целью в системе Windows Server используются динамические диски?

44. Для какой цели служит резервное копирование данных?

45. Какой есть режим резервного копирования, минимизирующий время восстановления данных?

46. На какие носители информации осуществляет резервное копирование система Windows Server?

47. Какой есть режим резервного копирования, минимизирующий объём архивируемых данных.?

48. Что делает функция технологии RAID ?

49. Как называется ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст?

50. Какие есть механизмы защиты информационных систем от несанкционированного доступа?

Составил преподаватель _____Скряго О.С.

Рассмотрено на заседании МК компьютерных сетей и администрирования
Протокол № 1 от 31.08.2023г
Председатель МК_____О.С. Скряго