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 МДК02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты
для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Промежуточная аттестация по МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты проходит в 5 семестре и 6 семестр. В 5 семестре формой промежуточной аттестации является другая форма аттестации в виде тестирования.

В 6 семестре форма промежуточной аттестации - это дифференцированный зачет. Дифференцируемый зачет подводит итог освоения МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты.

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.

Другие формы аттестации по МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты проводится в форме тестирования. К тестированию допускаются студенты, которые выполнили и защитили все лабораторно-практические занятия.

Тест содержит 10 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блоков (состоящих первый блок 30 вопросов, второй блок 20 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
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 ОК 01, ОК2, ОК3, ОК9, ПК 2.1, ПК 2.2 , ПК 2.3

№	ПК	Формулировка вопроса	Варианты ответов
1	ПК 2.1 ПК2.2 ПК 2.3	Как называется процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации?	1. Авторизация 2. Обезличивание 3. Деперсонализация 4. Аутентифика́ция 5. Идентификация
2	ПК 2.1 ПК2.2 ПК 2.3	Как называется процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом?	1. Авторизация 2. Обезличивание 3. Деперсонализация 4. Аутентифика́ция 5. Идентификаци
3	ПК2.3	Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя. Как данный идентификатор называется?	1. Токен 2. Password 3. Пароль 4. Login 5. Смарт-карта
4	ПК2.2 ПК 2.3	Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:	1. Идентификация 2. Аутентификация 3. Авторизация 4. Экспертиза 5. Шифрование
5	ПК 2.1 ПК 2.2 ПК 2.3	Для безопасной передачи данных по каналам интернет как используется технология?	1. WWW 2. DICOM 3. VPN 4. FTP 5. XML
6	ПК 2.1 ПК2.2 ПК 2.3	Как называется комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа?	1. Антивирус 2. Замок 3. Брандма́уэр 4. Криптография 5. Экспертная система

7	ПК 2.3	Для того чтобы снизить вероятность утраты информации, что необходимо сделать?	1. Регулярно производить антивирусную проверку компьютера 2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок 3. Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты) 4. Защитить вход на компьютер к данным паролем 5. Проводить периодическое обслуживание ПК
8	ПК 2.3	Какой пароль должен быть пользователем?	1. Содержать цифры и буквы, знаки препинания и быть сложным для угадывания 2. Содержать только цифры 3. Содержать только буквы 4. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.) 5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.
9	ПК 2.1 ПК2.2	Как называется устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающие маленький пейджер, не подсоединяемые к компьютеру и имеющие собственный источник питания?	1. Токен 2. Автономный токен 3. USB-токен 4. Устройство ibutton 5. Смарт-карта
10	ПК2.2 ПК 2.3	Как называется пластиковая карточка, содержащая чип для криптографических вычислений и встроенную защищенную память для хранения информации?	1. Токен 2. Password 3. Пароль 4. Login 5. Смарт-карта
11	ПК 2.1 ПК2.2 ПК 2.3	Доступ пользователя к информационным ресурсам компьютера и / или локальной вычислительной сети предприятия должен разрешаться только после, каких процессов?	1. Включения компьютера 2. Идентификации по логину и паролю 3. Запроса паспортных

			данных 4. Запроса доменного имени 5. Запроса ФИО
12	ПК 2.1	Виртуальная частная сеть - это метод, что позволяет? (выберите подходящий ответ)	1. Посредством беспроводной сети Wi-Fi организовать более безопасное соединение между всеми компонентами сети 2. Воспользоваться общедоступной телекоммуникационной инфраструктурой для предоставления удаленным офисам или отдельным пользователям безопасного доступа к сети организации 3. Обычным пользователям, не подключенным к Wi-Fi сети, обмениваться информацией через Internet
13	ПК 2.1 ПК 2.3	Для защиты от злоумышленников необходимо, что использовать?	1. Системное программное обеспечение 2. Прикладное программное обеспечение 3. Антивирусные программы 4. Компьютерные игры 5. Музыку, видеофильмы
14	ПК 2.1	Что определяет VPN?	1. базовую станцию беспроводной сети 2. сервер проводной сети Ethernet 3. виртуальную частную сеть
15		VPN и беспроводные технологии, что делают?	1. образуют неразрывную связь, без которой невозможно нормальное функционирование беспроводной сети 2. конкурируют между собой 3. не конкурируют, а дополняют друг друга

16	ПК 2.1 ПК2.2	Что определяет L2TP?	1. протокол на информационном уровне 2. туннельный протокол на канальном уровне 3. метод взаимодействия протоколов
17	ПК 2.1 ПК 2.2	Каким условиям отвечает VPN? (Выберите несколько правильных ответов)	1. целостности 2. мобильности 3. доступности 4. дорогая установки и настройка 5. конфиденциальности
18	ПК 2.1	Какие основные способы классификации VPN Вы знаете? (Выберите несколько правильных ответов)	1."сеть-хост-сеть" 2. "сеть-пользователь" 3. "сеть-сеть" 4. "хост-сеть" 5. "хост-хост"
19	ПК 2.2	При использовании топологии "хост-хост", что происходит?	1. удаленные пользователи подключаются к корпоративной сети через Internet 2. два хоста обменивающихся друг с другом шифрованными и нешифрованными данными. Туннель организуется между двумя хостами и весь трафик между ними инкапсулируется внутри VPN 3. два хоста обмениваются друг с другом нешифрованными данными и поэтому при такой топологии резко возрастает вероятность атак любых видов
20	ПК 2.1 ПК2.2	Протокол IPSec состоит, из каких основных частей? (Выберите несколько правильных ответов)	1. базовой основы инициализации 2. схемы обмена ключами через Internet 3. заголовка

			аутентификации 4. ключа проверки данных 5. безопасно инкапсулированной полезной нагрузки
21	ПК 2.1 ПК2.2	Что обеспечивает AH?	1. аутентификацию на уровне пакета и целостность данных 2. конфиденциальность, аутентификацию источника данных, целостность, опциональную защиту от атаки повторного сеанса и до некоторой степени скрытность механизма управления потоком 3. согласование настроек служб безопасности между сторонами-участниками
22	ПК 2.1 ПК2.2	Что обеспечивает IKE?	1. конфиденциальность, аутентификацию источника данных, целостность, опциональную защиту от атаки повторного сеанса и до некоторой степени скрытность механизма управления потоком 2. согласование настроек служб безопасности между сторонами-участниками 3. аутентификацию на уровне пакета и целостность данных
23	ПК 2.1	Что определяет IDS?	1. систему обнаружения вторжения 2. сетевые системы обнаружения вторжения 3. системы обнаружения вторжения на базе

			хоста
24	ПК 2.1 ПК 2.2 ПК 2.3	Системы обнаружения вторжения - это устройства, с помощью которых, что делают?: (продолжить определение)	1. нельзя своевременно выявить и предотвращать вторжения в вычислительные сети. Можно лишь определить факт вторжения по log-файлам 2. достигается наибольшая безопасность работы системы без вмешательства пользователей 3. можно выявлять и своевременно предотвращать вторжения в вычислительные сети
25	ПК 2.1 ПК 2.2 ПК 2.3	На какие виды делаться системы обнаружения вторжения? (Выберите несколько правильных ответов)	1. узконаправленные на базе конкретных сетевых атак 2. многоуровневые на базе секретных ключей 3. на базе идентификатора пользователя 4. на базе сети 5. на базе хоста
26	ПК 2.1 ПК 2.2 ПК 2.3	Что определяет NIDS?	1. сетевые системы обнаружения вторжения 2. систему обнаружения вторжения 3. системы обнаружения вторжения на базе хоста
27	ПК 2.1 ПК2.2	Протокол PPTP определяет несколько типов коммуникаций. Одним из таких типов является PPTP-туннель, который используется для чего? (продолжить высказывание)	1. обмена клиентом и сервером зашифрованными данными 2. обмена клиентом и сервером исходными, незашифрованными данными 3. поддержки соединения клиентов во время

			сетевых атак
28	ПК 2.1 ПК2.2	Какими бывают системы обнаружения вторжений? (Выберите несколько правильных ответов)	1. комбинированными 2. сетевыми 3. хостовыми
29	ПК 2.3	От каких атак сетевая система обнаружения вторжений может защитить? (Выберите несколько правильных ответов)	1. проходят через межсетевой экран во внутреннюю ЛВС 2. исходят из внутренней ЛВС во внешние сети 3. протекают в пределах внутренней ЛВС
30	ПК 2.1 ПК2.2	Основным методом, применяемым в сетевых системах обнаружения вторжений, является исследование проходящего трафика и чего еще?: (продолжить высказывание)	1. ввод полученных данных в самообучающиеся нейронные сети 2. сравнение его с базой данных известных шаблонов вредоносной активности 3. сравнение его статистических характеристик с профилями нормальной активно

Второй блок

Формируемые компетенции ОК1, ОК2, ОК3, ОК9, ПК2.1. ПК 2.2, ПК 2.3

1 . Что такое цель прогресса внедрения и тестирования средств защиты?

2. Как называется выделения пользователем и администраторам только тех прав доступа, которые им необходимы?

3. Какой недостаток систем шифрования с открытым ключом?

4. Как называется процесс запись определенных событий в журнал безопасности сервера?

5. Что называется конфигурацией из нескольких компьютеров, выполняющих общее приложение?

6. Что называют оконечным устройством канала связи, через которое процесс может передавать или получать данные?

7. Как называется получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля?

8. Как называются преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на ИС?

9. Чем обеспечивается защита исполняемых файлов?

10. Чем обеспечивается защита от программных закладок.

11. Чем обеспечивается защита от форматирования жесткого диска со стороны пользователей

12. Какой уровень ОС связан с доступом к информационным ресурсам внутри организации?

13. Что является сетевой службой, предназначенной для централизованного решения задач аутентификации и авторизации в крупных сетях?

14. "Уполномоченные серверы" были созданы для решения проблемы. Что это?

15. "Уполномоченные серверы" фильтруют пакеты на уровне. Что это?

16. ACL-список ассоциируется с каждым

17. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности. Что это?

18. На каком уровне модели взаимодействия открытых систем реализуются битовые протоколы передачи данных?

19. Что представляли собой брандмауэры второго поколения?

20. Что представляли собой брандмауэры первого поколения?

Дифференцированный зачет по МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты проводится в форме тестирования. К тестированию допускаются студенты, которые выполнили и защитили все лабораторно-практические занятия

Тест содержит 10 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блоков (состоящих первый блок 70 вопросов, второй блок 55 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
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 ОК 01, ОК2, ОК3, ОК9, ПК 2.1, ПК 2.2 , ПК 2.3

№	ПК	Формулировка вопроса	Варианты ответов
1	ПК 2.1 ПК2.2 ПК 2.3	Как называется процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации?	1. Авторизация 2. Обезличивание 3. Деперсонализация 4. Аутентифика́ция 5. Идентификация
2	ПК 2.1 ПК2.2 ПК 2.3	Как называется процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение	1. Авторизация 2. Обезличивание 3. Деперсонализация 4. Аутентифика́ция

		некоторых (разрешенных ему) действий в системах с ограниченным доступом?	5. Идентификаци
3	ПК2.3	Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя. Как данный идентификатор называется?	1. Токен 2. Password 3. Пароль 4. Login 5. Смарт-карта
4	ПК2.2 ПК 2.3	Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:	1. Идентификация 2. Аутентификация 3. Авторизация 4. Экспертиза 5. Шифрование
5	ПК 2.1 ПК 2.2 ПК 2.3	Для безопасной передачи данных по каналам интернет как используется технология?	1. WWW 2. DICOM 3. VPN 4. FTP 5. XML
6	ПК 2.1 ПК2.2 ПК 2.3	Как называется комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа?	1. Антивирус 2. Замок 3. Брандма́уэр 4. Криптография 5. Экспертная система
7	ПК 2.3	Для того чтобы снизить вероятность утраты информации, что необходимо сделать?	1. Регулярно производить антивирусную проверку компьютера 2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок 3. Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты) 4. Защитить вход на компьютер к данным паролем 5. Проводить периодическое обслуживание ПК
8	ПК 2.3	Какой пароль должен быть пользователем?	1. Содержать цифры и буквы, знаки препинания и быть сложным для угадывания 2. Содержать только цифры 3. Содержать только буквы 4. Иметь явную

			привязку к владельцу (его имя, дата рождения, номер телефона и т.п.) 5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.
9	ПК 2.1 ПК2.2	Как называется устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающие маленький пейджер, не подсоединяемые к компьютеру и имеющие собственный источник питания?	1. Токен 2. Автономный токен 3. USB-токен 4. Устройство ibutton 5. Смарт-карта
10	ПК2.2 ПК 2.3	Как называется пластиковая карточка, содержащая чип для криптографических вычислений и встроенную защищенную память для хранения информации?	6. Токен 7. Password 8. Пароль 9. Login 10. Смарт-карта
11	ПК 2.1 ПК2.2 ПК 2.3	Доступ пользователя к информационным ресурсам компьютера и / или локальной вычислительной сети предприятия должен разрешаться только после, каких процессов?	1. Включения компьютера 2. Идентификации по логину и паролю 3. Запроса паспортных данных 4. Запроса доменного имени 5. Запроса ФИО
12	ПК 2.1	Виртуальная частная сеть - это метод, что позволяет? (выберите подходящий ответ)	4. Посредством беспроводной сети Wi-Fi организовать более безопасное соединение между всеми компонентами сети 5. Воспользоваться общедоступной телекоммуникационной инфраструктурой для предоставления удаленным офисам или отдельным пользователям безопасного доступа к сети организации 6. Обычным пользователям, не подключенным к Wi-Fi сети, обмениваться информацией через Internet

13	ПК 2.1 ПК 2.3	Для защиты от злоумышленников необходимо, что использовать?	1. Системное программное обеспечение 2. Прикладное программное обеспечение 3. Антивирусные программы 4. Компьютерные игры 5. Музыку, видеофильмы
14	ПК 2.1	Что определяет VPN?	4. базовую станцию беспроводной сети 5. сервер проводной сети Ethernet 6. виртуальную частную сеть
15		VPN и беспроводные технологии, что делают?	1. образуют неразрывную связь, без которой невозможно нормальное функционирование беспроводной сети 2. конкурируют между собой 3. не конкурируют, а дополняют друг друга
16	ПК 2.1 ПК2.2	Что определяет L2TP?	4. протокол на информационном уровне 5. туннельный протокол на канальном уровне 6. метод взаимодействия протоколов
17	ПК 2.1 ПК 2.2	Каким условиям отвечает VPN? (Выберите несколько правильных ответов)	6. целостности 7. мобильности 8. доступности 9. дорогая установки и настройка 10. конфиденциальности
18	ПК 2.1	Какие основные способы классификации VPN Вы знаете? (Выберите несколько правильных ответов)	1."сеть-хост-сеть" 2. "сеть-пользователь" 3. "сеть-сеть" 4. "хост-сеть" 5. "хост-хост"
19	ПК 2.2	При использовании топологии "хост-хост", что происходит?	4. удаленные пользователи подключаются к корпоративной сети через Internet 5. два хоста

			обменивающихся друг с другом шифрованными и нешифрованными данными. Туннель организуется между двумя хостами и весь трафик между ними инкапсулируется внутри VPN 6. два хоста обмениваются друг с другом нешифрованными данными и поэтому при такой топологии резко возрастает вероятность атак любых видов
20	ПК 2.1 ПК2.2	Протокол IPSec состоит, из каких основных частей? (Выберите несколько правильных ответов)	6. базовой основы инициализации 7. схемы обмена ключами через Internet 8. заголовка аутентификации 9. ключа проверки данных 10. безопасно инкапсулированной полезной нагрузки
21	ПК 2.1 ПК2.2	Что обеспечивает АН?	4. аутентификацию на уровне пакета и целостность данных 5. конфиденциальность, аутентификацию источника данных, целостность, опциональную защиту от атаки повторного сеанса и до некоторой степени скрытность механизма управления потоком 6. согласование настроек служб безопасности между сторонами-участниками
22	ПК 2.1	Что обеспечивает IKE?	4. конфиденциальн

	ПК2.2		ость, аутентификацию источника данных, целостность, опциональную защиту от атаки повторного сеанса и до некоторой степени скрытность механизма управления потоком 5. согласование настроек служб безопасности между сторонами-участниками 6. аутентификацию на уровне пакета и целостность данных
23	ПК 2.1	Что определяет IDS?	4. систему обнаружения вторжения 5. сетевые системы обнаружения вторжения 6. системы обнаружения вторжения на базе хоста
24	ПК 2.1 ПК 2.2 ПК 2.3	Системы обнаружения вторжения - это устройства, с помощью которых, что делают?: (продолжить определение)	4. нельзя своевременно выявить и предотвращать вторжения в вычислительные сети. Можно лишь определить факт вторжения по log-файлам 5. достигается наибольшая безопасность работы системы без вмешательства пользователей 6. можно выявлять и своевременно предотвращать вторжения в вычислительные сети
25	ПК 2.1 ПК 2.2 ПК 2.3	На какие виды делаться системы обнаружения вторжения? (Выберите несколько правильных ответов)	6. узконаправленные на базе конкретных сетевых атак 7. многоуровневые на базе секретных ключей 8. на базе идентификатора

			пользователя 9. на базе сети 10. на базе хоста
26	ПК 2.1 ПК 2.2 ПК 2.3	Что определяет NIDS?	4. сетевые системы обнаружения вторжения 5. систему обнаружения вторжения 6. системы обнаружения вторжения на базе хоста
27	ПК 2.1 ПК2.2	Протокол PPTP определяет несколько типов коммуникаций. Одним из таких типов является PPTP-туннель, который используется для чего? (продолжить высказывание)	4. обмена клиентом и сервером зашифрованными данными 5. обмена клиентом и сервером исходными, незашифрованными данными 6. поддержки соединения клиентов во время сетевых атак
28	ПК 2.1 ПК2.2	Какими бывают системы обнаружения вторжений? (Выберите несколько правильных ответов)	4. комбинированными 5. сетевыми 6. хостовыми
29	ПК 2.3	От каких атак сетевая система обнаружения вторжений может защитить? (Выберите несколько правильных ответов)	4. проходят через межсетевой экран во внутреннюю ЛВС 5. исходят из внутренней ЛВС во внешние сети 6. протекают в пределах внутренней ЛВС
30	ПК 2.1 ПК2.2	Основным методом, применяемым в сетевых системах обнаружения вторжений, является исследование проходящего трафика и чего еще?: (продолжить высказывание)	4. ввод полученных данных в самообучающиеся нейронные сети 5. сравнение его с базой данных известных шаблонов вредоносной активности 6. сравнение его статистических характеристик с

			профилями нормальной активно
31	ПК 2.1 ПК2.2	Как называется шаблон вредоносной активности?	1. идентификационной меткой 2. подписью 3. профилем 4.сигнатурой 5. цифровым отпечатком
32	ПК 2.1 ПК2.2 ПК 2.3	Основным методом, применяемым в хостовых системах обнаружения вторжений, что является? (продолжить высказывание)	1. контроль целостности ключевых файлов 2. сравнение статистических характеристик поведения пользователей с профилями нормальной активности 3. сравнение статистических характеристик поведения программ с профилями нормальной активности
33	ПК 2.1 ПК2.2 ПК 2.3	Перечислите основные достоинства систем обнаружения вторжений на основе выявления аномальной активности. (Выберите несколько правильных ответов)	1. возможность обнаружения неизвестных ранее видов атак 2. отсутствие ложных срабатываний 3. отсутствие необходимости постоянного обновления сигнатур
34	ПК 2.1 ПК2.2	Какие Вы знаете основными недостатками систем обнаружения вторжений на основе выявления аномальной активности? (Выберите несколько правильных ответов)	1. большое число ложных срабатываний 2. длительность и сложность определения профилей нормальной активности 3. пропуск атак, статистические характеристики которых близки к нормальным
35	ПК 2.1	Основная идея сетевых систем предотвращения	1. запрос систем-

		вторжений состоит в том, чтобы при генерации тревожных сигналов предпринимать ответные действия, какого рода? (Выберите несколько правильных ответов)	нарушителей 2. контратака систем-нарушителей 3. написание "на лету" индивидуальных правил для межсетевых экранов и маршрутизаторов, блокирующих активность подозрительных IP-адресов
36	ПК 2.1 ПК2.2	Какие главные проблемы систем обнаружения вторжений Вы знаете? (Выберите несколько правильных ответов)	1. большое число ложных срабатываний 2. проблематичность работы в реальном масштабе времени 3. пропуск неизвестных атак
37	ПК 2.1 ПК2.2	Что относиться к ложным срабатываниям сетевых систем обнаружения вторжений?	1. максимальная подозрительность подразумеваемой конфигурации 2.минимальная подозрительность подразумеваемой конфигурации 3. отсутствие обновлений в подразумеваемой конфигурации
38	ПК 2.1 ПК2.2	Какие причины принадлежат к сложным срабатываниям сетевых систем обнаружения вторжений? (Выберите несколько правильных ответов)	1. работа системы мониторинга сети 2. работа системы резервного копирования 3. работа системы сетевого управления
39	ПК 2.1 ПК2.2 ПК 2.3	Что относиться к числу типичных причин ложных срабатываний сетевых систем обнаружения вторжений? (Выберите несколько правильных ответов)	1. работа межсетевого экрана 2. работа сетевого сканера уязвимостей 3. работа сканера портов

40	ПК 2.1 ПК2.2 ПК 2.3	Что относиться к числу типичных причин срабатываний сетевых систем обнаружения вторжений? (Выберите несколько правильных ответов)	1. пользовательская активность в виде использования потокового видео 2. пользовательская активность в виде мгновенного обмена сообщениями 3. пользовательская активность в виде однорангового разделения файлов
41	ПК 2.1 ПК2.2 ПК 2.3	Что принадлежит к числу типичных причин ложных срабатываний сетевых систем обнаружения вторжений?	1. параллельное применение нескольких сетевых систем обнаружения вторжений 2. параллельное применение сетевых и хостовых систем обнаружения вторжений 3. применение программ, поведение которых напоминает троянскую программу или черв
42	ПК 2.1	Какие программы пытаются копировать на различные системы файлы с расширением .eml? (Выберите несколько правильных ответов)	1. программа Microsoft Exchange при использовании ее Web-интерфейса 2. программа Microsoft Word при преобразовании документа в .eml-файл 3. червь Nimda
40	ПК 2.1 ПК2.2 ПК 2.3	Что принадлежит к числу типичных причин ложных срабатываний сетевых систем обнаружения вторжений? (Выберите несколько правильных ответов)	1. активное администрирование баз данных 2. длинные базовые цепочки аутентификации 3. применение длинных и сложных паролей
43	ПК 2.1 ПК2.2	Что необходимо чтобы реализовать потенциал системы обнаружения вторжений? (Выберите несколько правильных ответов)	1. быть специалистом по математической статистике 2. выполнить правильное конфигурирование системы

			3. загрузить файлы системы обнаружения вторжений
44	ПК 2.1 ПК2.2	Что необходимо чтобы реализовать потенциал системы обнаружения вторжений? (Выберите несколько правильных ответов)	1. задействовать средства анализа для систем обнаружения вторжений 2. круглосуточно принимать, анализировать и реагировать на сигналы тревоги, генерируемые системой обнаружения вторжений 3. оперативно обновлять базу сигнатур
45	ПК 2.1 ПК2.2 ПК 2.3	Что необходимо чтобы реализовать потенциал системы обнаружения вторжений? (Выберите несколько правильных ответов)	1. выяснить характер нормального трафика в сети 2. осуществить настройку системы обнаружения вторжений 3. установить систему обнаружения вторжений
46	ПК 2.1 ПК2.2 ПК 2.3	Что необходимо, чтобы минимизировать число ложных срабатываний системы обнаружения вторжений?	1. индивидуализироват ь настройки для своей сети 2.использовать подразумеваемые настройки 3. минимизировать число настраиваемых параметров
47	ПК 2.1 ПК2.2 ПК 2.3	Что предпочтительно выполнять, чтобы минимизировать число ложных срабатываний системы обнаружения вторжений?	1.выполнить упреждающее конфигурирование 2.не изменять конфигурацию сети 3.перенастроить систему постфактум
48	ПК 2.1 ПК2.2	Большинство систем обнаружения вторжений группируют сигналы тревоги, по какому типу?: (продолжить высказывание)	1. категориям 2. по размеру возможного ущерба от

			успешной атаки 3. по степени критичности атакуемых систем
49	ПК 2.1 ПК2.2 ПК 2.3	Категорию сигналов тревоги для UNIX-платформ можно безопасно отключить, при каких условиях?: (продолжить высказывание)	1.в сети нет UNIX-систем 2.вы уверены в безопасности UNIX-систем 3. длительное время не генерируются сигналы тревоги для UNIX-систем
50	ПК 2.1 ПК2.2 ПК 2.3	Когда сигналы тревоги по поводу использования мгновенного обмена сообщениями можно безопасно отключить? (Выберите несколько правильных ответов)	1. вы уверены в безвредности мгновенного обмена сообщениями 2. есть другие системы, фильтрующие подобные виды активности 3. политика безопасности разрешает подобные виды активности
51	ПК 2.1 ПК2.2 ПК 2.3	Когда сигналы тревоги по поводу использования однорангового разделения файлов можно безопасно отключить? (Выберите несколько правильных ответов)	1. вы уверены в безвредности однорангового разделения файлов 2. есть другие системы, фильтрующие подобные виды активности 3.политика безопасности разрешает подобные виды активности
52	ПК 2.1 ПК 2.2 ПК 2.3	Чтобы минимизировать число ложных срабатываний сетевой системы обнаружения вторжений, что можно делать?: (продолжить высказывание)	1.освободить направляемый вовне трафик от контроля 2. освободить некоторые хосты от контроля 3.освободить некоторых пользователей от контроля
53	ПК 2.1 ПК 2.2 ПК 2.3	Что происходит при освобождении хостов от контроля со стороны сетевой системы обнаружения вторжений? (Выберите несколько правильных ответов)	1.может оставить критически важные машины без защиты 2. снижает уровень безопасности

			3.способно сделать работу администратора безопасности более эффективной
54	ПК 2.1 ПК 2.2	Какие недостатков хостовых методов обнаружения вторжений Вы знаете? (Выберите несколько правильных ответов)	1.большая уязвимость самой системы обнаружения вторжений 2.необходимость загрузки и управления программным обеспечением на каждой защищаемой машине 3.сигналы тревоги поступают после успешной атаки; сетевые системы обнаружения вторжений обеспечивают иногда более раннее предупреждение
55	ПК 2.1 ПК 2.2	Для контроля чего применяются хостовые системы обнаружения вторжений?	1. всей информационной системы организации 2.клиентских машин 3. критически важных серверов
56	ПК 2.1 ПК 2.2	Какие преимуществ хостовых методов обнаружения вторжений Вы знаете? (Выберите несколько правильных ответов)	1. не требуется постоянное обновление сигнатур, поскольку отслеживаются проявления активности, а не сигнатуры 2. одна система контролирует большее число машин 3.они требуют меньше обслуживания и настройки
57	ПК 2.1 ПК 2.2	Какие преимуществ хостовых методов обнаружения вторжений перед сетевыми Вы знаете? (Выберите несколько правильных ответов)	1. они лучше приспособлены для работы в реальном масштабе времени 2. они генерируют меньшее число ложных срабатываний 3. они менее подвержены обману

58	ПК 2.1 ПК 2.2	По сравнению с сетевыми, хостовые системы обнаружения вторжений, основанные на контроле целостности аппаратно-программной конфигурации, что генерируют?	1. больше ложных срабатываний 2. меньше ложных срабатываний 3. примерно столько же ложных срабатываний
59	ПК 2.1 ПК 2.2 ПК 2.3	Какие признаки компрометации хоста Вы знаете? (Выберите несколько правильных ответов)	1. изменение режима доступа к файлам 2.изменение режима работы пользователей 3. изменение системных конфигурационных файлов
60	ПК 2.1 ПК 2.2	Какие признаки компрометации хоста Вы знаете? (Выберите несколько правильных ответов)	1. добавление пользователей 2. модификация файла паролей 3. пополнение регистрационных журналов
61	ПК 2.1 ПК 2.2	Какой признак компрометации хоста Вы знаете?	1.изменение занятого дискового пространства 2. изменение определенных системных файлов 3. изменение пользовательских файлов
62	ПК 2.1 ПК 2.2 ПК 2.3	Что необходимо для Snort for Windows? (Выберите несколько правильных ответов)	1. база данных MySQL 2. мощная аппаратура 3. установленные библиотеки WinPcap 4. установленный сервер IIS
63	ПК 2.1 ПК 2.2 ПК 2.3	Что целесообразно сделать, чтобы смягчить проблемы, присущие размещению сетевой системы обнаружения вторжений между поставщиком Интернет-услуг и межсетевым экраном? (Выберите несколько правильных ответов)	1. максимально расширить спектр генерируемых сигналов тревоги 2. ограничиться сигналами тревоги, отражающими специфику вашего сетевого сегмента 3.сократить число сигнатур до небольшой величины 4. увеличить число

			сигнатур
64	ПК 2.1 ПК 2.2 ПК 2.3	К числу недостатков размещения сетевой системы обнаружения вторжений между поставщиком Интернет-услуг и межсетевым экраном принадлежат, что является?	1. ее база правил может стать слишком большой 2.она будет требовать постоянного обновления сигнатур 3.она может стать одиночной точкой отказа для сетевого трафика
65	ПК 2.1 ПК 2.2 ПК 2.3	Какие достоинства размещения сетевой системы обнаружения вторжений между поставщиком Интернет-услуг и межсетевым экраном Вы знаете? (Выберите несколько правильных ответов)	1.возможность защитить межсетевой экран от внешних атак 2.возможность защитить межсетевой экран от внутренних атак 3.возможность перехватывать все, что направлено против общедоступных серверов и внутренней ЛВС 4. возможность фильтровать весь входящий и исходящий трафик ЛВС и демилитаризованной зоны
66	ПК 2.1 ПК 2.2 ПК 2.3	Что необходимо сделать, чтобы сетевая система обнаружения вторжений была эффективным средством защиты общедоступных серверов? (Выберите несколько правильных ответов)	1. ввести специальные правила с учетом семантики предоставляемых сервисов 2.контролировать административные входы в серверные системы 3.разместить сенсоры сетевой системы обнаружения вторжений перед межсетевым экраном
67	ПК 2.1 ПК 2.2 ПК 2.3	Какую активность позволяет отслеживать размещение сетевой системы обнаружения вторжений в демилитаризованной зоне? (Выберите несколько правильных ответов)	1. межсетевого экрана по отношению к общедоступным серверам 2. общедоступных серверов по отношению к внешним пользователям 3. общедоступных серверов по отношению к внутренним

			пользователям 4.общедоступных серверов по отношению к межсетевому
68	ПК 2.1 ПК 2.2 ПК 2.3	Размещение сетевой системы обнаружения вторжений в демилитаризованной зоне позволяет отслеживать активность чего?	1. внутренних пользователей по отношению к общедоступным серверам 2.внутренних пользователей по отношению к межсетевому экрану 3. внутренних пользователей по отношению к локальной сети
69	ПК 2.1 ПК 2.2 ПК 2.3	Какой из компонентов подсистемы безопасности Windows предназначен для контроля за доступом к объектам?	1. Encrypted File Syste 2. NT File System 3. Security Account Manager 4. Security Reference Monitor
70	ПК 2.1 ПК 2.2	К какому типу протоколов относится протокол SSL?	1.К протоколам прямой аутентификации 2. К протоколам автономной аутентификации 3. К протоколам установления защищенной связи на сетевом уровне 4. К протоколам непрямой аутентификации

Второй блок

Формируемые компетенции ОК1, ОК2, ОК3, ОК9, ПК2.1. ПК 2.2, ПК 2.3

1 . Что такое цель прогресса внедрения и тестирования средств защиты?

2. Как называется выделения пользователем и администраторам только тех прав доступа, которые им необходимы?

3. Какой недостаток систем шифрования с открытым ключом?

4. Как называется процесс запись определенных событий в журнал безопасности сервера?

5. Что называется конфигурацией из нескольких компьютеров, выполняющих общее приложение?

6. Что называют оконечным устройством канала связи, через которое процесс может передавать или получать данные?

7. Как называется получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля?

8. Как называются преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на ИС?

9. Чем обеспечивается защита исполняемых файлов?

10. Чем обеспечивается защита от программных закладок.

11. Чем обеспечивается защита от форматирования жесткого диска со стороны пользователей

12. Какой уровень ОС связан с доступом к информационным ресурсам внутри организации?

13. Что является сетевой службой, предназначенной для централизованного решения задач аутентификации и авторизации в крупных сетях?

14. "Уполномоченные серверы" были созданы для решения проблемы. Что это?

15. "Уполномоченные серверы" фильтруют пакеты на уровне. Что это?

16. ACL-список ассоциируется с каждым

17. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности. Что это?

18. На каком уровне модели взаимодействия открытых систем реализуются битовые протоколы передачи данных?

19. Что представляли собой брандмауэры второго поколения?

20. Что представляли собой брандмауэры первого поколения?

21. Для фильтрации чего используют брандмауэры третьего поколения?

22. Что за действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели?

23. Что подразделяется в соответствии с видами объектов привилегии доступа?

25. Для разграничения доступа к файлу применяются флаги, разрешающие что?

26. Как может рассматриваться доступ к объекту в многоуровневой модели?

27. На каком уровне модели взаимодействия открытых систем реализуются маршрутизация и управление потоками данных?

28. Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты за что?

29. На каком уровне ОС происходит определение допустимых для пользователя ресурсов ОС?

30. Чем определяется надежность СЗИ?

31. Что такое гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные?

32. Что такое политика информационной безопасности?

33. Что такое предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы?

34. Что такое присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации?

35. Что такое проверка подлинности пользователя по предъявленному им идентификатору?

36. Что такое проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы?

37. Что такое свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов.

38. Что такое степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования?

39. Что такое троянские программы?

40. Что занимается обеспечением скрытности информации в информационных массивах?

41. Как называется метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации?

42. Что называется нормативным документом, регламентирующим все аспекты безопасности продукта информационных технологий?

43. Что называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения?

44. Что называется процессом имитации хакером дружественного адреса?

45. Что называется системой, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую?

46. Что называется списком объектов, к которым может быть получен доступ, вместе с доменом защиты объекта.?

47. Что называется удачной криптоатакой.

48. Что объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей?

49. Что составляет основу политики безопасности?

50. Что является первым этапом разработки системы защиты ИС?

51. Что являются достоинствами аппаратной реализации криптографического закрытия данных?

52. Что являются достоинствами программной реализации криптографического закрытия данных?

53. Что являются аспектами адекватности средств защиты?

54. Что включает процесс анализа рисков при разработке системы защиты ИС?

55. Что различает модели воздействия программных закладок на компьютеры?

Составил преподаватель Скряго О.С.