Утверждаю
Зам. директора по УР
«28» 06 2024г.
Иванешко И.В.

Согласовано
Главный специалист по защите информации
ООО «БИРСЕК»
«28» 06 2024г.
А.А. Ефремов

Контрольно-оценочные средства для промежуточной аттестации по МДК.03.02 Технологии автоматизации технологических процессов, МДК.03.03 Безопасность компьютерных сетей
по специальности 09.02.06 Сетевое и системное администрирование

Промежуточная аттестация по МДК.03.02 Технологии автоматизации технологических процессов, МДК.03.03 Безопасность компьютерных сетей - это комплексны дифференцированный зачет. Комплексный дифференцированный зачет является промежуточной формой контроля, подводит итог освоения МДК.03.02 Технологии автоматизации технологических процессов, МДК.03.03 Безопасность компьютерных сетей.

Профессиональные компетенции:
ПК 3.1. Осуществлять проектирование сетевой инфраструктуры.
ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств.
ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств.
ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.
ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем.
ПК 2.3. Осуществлять сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.
ПК 2.4. Осуществлять проведение обновления программного обеспечения операционных систем и прикладного программного обеспечения.
ПК 2.5. Осуществлять выявление и устранение инцидентов в процессе функционирования операционных систем.

общих компетенций (ОК):
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02. Использовать современные средства поиска, анализ и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

Комплексный дифференцированный зачет по МДК.03.02 Технологии автоматизации технологических процессов, МДК.03.03 Безопасность компьютерных сетей проводится в форме тестирования.

К тестированию допускаются студенты при условии выполнения 95% лабораторных занятий на положительные оценки (оценки 3,4,5).

Тест содержит 20 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 10 вопросов. Время тестирования – 45 минут для каждой подгруппы (по 1,5 минуты на каждый вопрос из первого блока, по 3 минут на каждый вопрос закрытого типа).

Критерии оценивания
«5 баллов » - получают студенты, справившиеся с работой на 100-90%;
«4 балла » - ставится в том случае, если верные ответы составляют 89-70% от общего количества;

«3 балла » - соответствует работа, содержащая 50-69% правильных ответов;
«2 балла» - соответствует работа, содержащая менее 50% 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, ОК5, ПК 2.3- ПК 2.5, ПК 3.1-ПК3.5

№	ПК	Формулировка вопроса	Варианты ответов
1)	ПК 3.1 ПК3.2 ПК 3.5	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК3.2 ПК 3.3 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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)	ПК3.3 ПК 3.5 ПК 2.3 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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)	ПК3.2 ПК 3.3 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2 ПК 3.3	*Прочитайте текст и выберите правильный ответ.* Для безопасной передачи данных по каналам интернет как используется технология?	1. WWW. 2. DICOM. 3. VPN. 4. FTP. 5. XML.
6)	ПК 3.1 ПК 3.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 2.3 ПК 3.2	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.5 ПК 2.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК3.5 ПК 3.2 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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)	ПК3.4 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК3.2 ПК 3.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* Доступ пользователя к информационным ресурсам компьютера и / или локальной вычислительной сети предприятия должен разрешаться только после,	1. Включения компьютера. 2. Идентификации по логину и паролю.

		каких процессов?	3. Запроса паспортных данных. 4. Запроса доменного имени. 5. Запроса ФИО.
12)	ПК 3.1	*Прочитайте текст и выберите правильный ответ.* 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. 4. Обычным пользователям, не подключенным к Wi-Fi сети, обмениваться информацией через блютус.
13)	ПК 3.1 ПК 3.3	*Прочитайте текст и выберите правильный ответ.* 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 3.1	*Прочитайте текст и выберите правильный ответ.* Что определяет VPN?	1. Базовую станцию беспроводной сети. 2. Сервер проводной сети Ethernet. 3. Виртуальную частную сеть. 4. Частную сеть.
15)		*Прочитайте текст и выберите правильный ответ.* 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. 4. Взаимодействуют.
16)	ПК 3.1 ПК3.2 ПК 3.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* Что определяет L2TP?	1. Протокол на информационном уровне. 2. Туннельный протокол на канальном уровне. 3. Метод взаимодействия протоколов. 4. Метод удаления протоколов.
17)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 2.3 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* Каким условиям отвечает VPN? (Выберите несколько правильных ответов)	1. Целостности. 2. Мобильности. 3. Доступности. 4. дорогая установки и настройка. 5. Конфиденциальности.
18)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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 3.2 ПК 3.3 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Замена внутренней на внешнюю сеть.
20)	ПК 3.1 ПК3.2 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2 ПК 3.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* Что обеспечивает АН?	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. 4. Соглашение о неразглашении.
22)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 2.6	*Прочитайте текст и выберите правильный ответ.* 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. 4. Служба настройки домена.
23)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* Что определяет IDS?	1. Систему обнаружения вторжения. 2. Сетевые системы обнаружения вторжения. 3. Системы обнаружения вторжения на базе хоста. 4. Система доменных имен
24)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. Можно устраивать нападения извне.
25)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2	*Прочитайте текст и выберите правильный ответ.* Что определяет NIDS?	1. Сетевые системы обнаружения

	ПК 3.3 ПК 3.5		вторжения. 2. Систему обнаружения вторжения. 3. Системы обнаружения вторжения на базе хоста. 4. Система обнаружения домена.
27)	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Обмен деньгами.
28)	ПК 2.3 ПК2.4 ПК 3.5	*Прочитайте текст и выберите правильный ответ.* Какими бывают системы обнаружения вторжений? (Выберите несколько правильных ответов)	1. Комбинированным и. 2. Сетевыми. 3. Хостовыми. 4. Речными.
29)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Исходят по домену.
30)	ПК 3.1 ПК 3.2 ПК 3.3 ПК 2.5 ПК 2.6	*Прочитайте текст и выберите правильный ответ.* 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. 4. Сравнение доменных имен.
31)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* Как называется шаблон вредоносной активности?	1. Идентификационной меткой. 2. Подписью. 3. Профилем. 4.Сигнатурой. 5. Цифровым отпечатком.
32)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Сравнение доменов.
33)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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. 4. Отсутствие домена.
34)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. Пропуск доменных

			имен.
35)	ПК 3.1 ПК 3.3 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* Основная идея сетевых систем предотвращения вторжений состоит в том, чтобы при генерации тревожных сигналов предпринимать ответные действия, какого рода? (Выберите несколько правильных ответов)	1. Запрос систем-нарушителей. 2. Контратака систем-нарушителей. 3. Написание "на лету" индивидуальных правил для межсетевых экранов и маршрутизаторов, блокирующих активность подозрительных IP-адресов. 4. Контроль доменных имен.
36)	ПК 3.1 ПК 3.2 ПК 3.3 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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. 4. Пропуск домена.
37)	ПК 3.1 ПК 3.4 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. Отсутствие домена.
38)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 3.6	*Прочитайте текст и выберите правильный ответ.* 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. 4. Работа с доменами.
39)	ПК 3.1 ПК 3.4 ПК 3.5 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* Что относиться к числу типичных причин ложных срабатываний сетевых систем обнаружения вторжений? (Выберите несколько правильных	1. Работа межсетевого экрана. 2. Работа сетевого сканера

		ответов)	уязвимостей. 3. Работа сканера портов. 4. Работа с доменами.
40)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.3 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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. 4. Пользователь домена.
41)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 3.5 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Применение домена.
42)	ПК 3.1 ПК 3.2 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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. 4. Червь домена.
40)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. Применение домена.
43)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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. 4. Загрузить домен.
44)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Оператор домен.
45)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. Установить домен.
46)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* Что необходимо, чтобы минимизировать число ложных срабатываний системы обнаружения вторжений?	1. Индивидуализировать настройки для своей сети. 2.Использовать подразумеваемые

			настройки. 3. Минимизировать число настраиваемых параметров.
47)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* Что предпочтительно выполнять, чтобы минимизировать число ложных срабатываний системы обнаружения вторжений?	1.Выполнить упреждающее конфигурирование. 2.Не изменять конфигурацию сети. 3.Перенастроить систему постфактум. 4. Настроить домен.
48)	ПК 3.1 ПК 3.2 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. По домену.
49)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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. 4. В домен.
50)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Вы уверены в домене.
51)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 3.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Есть домен.
52)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. Освободить домен.
53)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 3.5 ПК 2.6	*Прочитайте текст и выберите правильный ответ.* 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. 4. Способно сделать домен.
54)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 3.5 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Сигналы домена.
55)	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* Для контроля чего применяются хостовые системы обнаружения вторжений?	1. Всей информационной системы организации. 2.Клиентских машин. 3. Критически важных

			серверов. 4. Критически важных доменов.
56)	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. Они генерируют домен.
58)	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК 2.6	*Прочитайте текст и выберите правильный ответ.* 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. 4. Примерно столько доменов.
59)	ПК 3.1 ПК 3.2 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2 ПК 3.3 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* Какие признаки компрометации хоста Вы знаете? (Выберите несколько правильных ответов)	1. Добавление пользователей. 2. Модификация файла паролей. 3. Пополнение регистрационных журналов. 4.Пополнение доменов.

61)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* Какой признак компрометации хоста Вы знаете?	1.Изменение занятого дискового пространства. 2. Изменение определенных системных файлов. 3.Изменение пользовательских файлов. 4. Изменение доменов.
62)	ПК 3.1 ПК 3.2 ПК 3.3 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2 ПК 3.5 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2 ПК 3.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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. 4. Она может в домен.
65)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 3.5	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2 ПК 3.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. Разместить домен.
67)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 2.5	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2 ПК 3.3 ПК 2.3	*Прочитайте текст и выберите правильный ответ.* 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. 4. Внутренних доменов.

69)	ПК 3.1 ПК 3.2 ПК 3.4 ПК 2.4	*Прочитайте текст и выберите правильный ответ.* 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 3.1 ПК 3.2	*Прочитайте текст и выберите правильный ответ.* 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 ОК 01, ОК2, ОК5, ПК 2.3- ПК 2.5

1) *Прочитайте текст и ответьте на вопрос.*

Что такое цель прогресса внедрения и тестирования средств защиты?

2) Прочитайте текст и ответьте на вопрос.

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

3) Прочитайте текст и ответьте на вопрос.

Какой недостаток систем шифрования с открытым ключом?

4) Прочитайте текст и ответьте на вопрос.

Как называется процесс запись определенных событий в журнал безопасности сервера?

5) *Прочитайте текст и ответьте на вопрос.*

Что называется конфигурацией из нескольких компьютеров, выполняющих общее приложение?

6) *Прочитайте текст и ответьте на вопрос.*

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

7) *Прочитайте текст и ответьте на вопрос.*

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

8) *Прочитайте текст и ответьте на вопрос*.

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

9) *Прочитайте текст и ответьте на вопрос*.

Чем обеспечивается защита исполняемых файлов?

10) *Прочитайте текст и ответьте на вопрос.*

Чем обеспечивается защита от программных закладок.

11) *Прочитайте текст и ответьте на вопрос.*

Чем обеспечивается защита от форматирования жесткого диска со стороны пользователей

12) *Прочитайте текст и ответьте на вопрос.*

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

13) *Прочитайте текст и ответьте на вопрос.*

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

14) *Прочитайте текст и ответьте на вопрос.*

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

15) *Прочитайте текст и ответьте на вопрос.*

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

16) *Прочитайте текст и ответьте на вопрос.*

ACL-список ассоциируется с каждым

17) *Прочитайте текст и ответьте на вопрос.*

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

18) *Прочитайте текст и ответьте на вопрос.*

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

19) *Прочитайте текст и ответьте на вопрос.*

Что представляли собой брандмауэры второго поколения?

20) *Прочитайте текст и ответьте на вопрос.*

Что представляли собой брандмауэры первого поколения?

21) *Прочитайте текст и ответьте на вопрос.*

Для фильтрации чего используют брандмауэры третьего поколения?

22) *Прочитайте текст и ответьте на вопрос.*

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

23) *Прочитайте текст и ответьте на вопрос.*

Что подразделяется в соответствии с видами объектов привилегии доступа?

25) *Прочитайте текст и ответьте на вопрос.*

Для разграничения доступа к файлу применяются флаги, разрешающие что?

Формируемые компетенции ОК 01, ОК2, ОК5, ПК 3.1, ПК 3.5, ПК 3.4

26) *Прочитайте текст и ответьте на вопрос.*
Как может рассматриваться доступ к объекту в многоуровневой модели?

27) *Прочитайте текст и ответьте на вопрос.*

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

28) *Прочитайте текст и ответьте на вопрос.*

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

29) *Прочитайте текст и ответьте на вопрос.*

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

30) *Прочитайте текст и ответьте на вопрос.*

Чем определяется надежность СЗИ?

31) *Прочитайте текст и ответьте на вопрос.*

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

32) *Прочитайте текст и ответьте на вопрос.*

Что такое политика информационной безопасности?

33) *Прочитайте текст и ответьте на вопрос.*

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

34) *Прочитайте текст и ответьте на вопрос.*

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

35) *Прочитайте текст и ответьте на вопрос.*

Что такое проверка подлинности пользователя по предъявленному им идентификатору?

36) *Прочитайте текст и ответьте на вопрос.*

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

37) *Прочитайте текст и ответьте на вопрос.*

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

38) *Прочитайте текст и ответьте на вопрос.*

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

39) *Прочитайте текст и ответьте на вопрос.*

Что такое троянские программы?

Формируемые компетенции ОК 01, ОК2, ОК5, ПК 3.2, ПК 3.3

40) *Прочитайте текст и ответьте на вопрос.*

Что занимается обеспечением скрытности информации в информационных массивах?

41) *Прочитайте текст и ответьте на вопрос.*

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

42) *Прочитайте текст и ответьте на вопрос.*

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

43) *Прочитайте текст и ответьте на вопрос.*

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

44) *Прочитайте текст и ответьте на вопрос.*

Что называется процессом имитации хакером дружественного адреса?

45) *Прочитайте текст и ответьте на вопрос.*

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) *Прочитайте текст и ответьте на вопрос.*

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

47) *Прочитайте текст и ответьте на вопрос.*

Что называется удачной криптоатакой.

48) *Прочитайте текст и ответьте на вопрос.*

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

49) *Прочитайте текст и ответьте на вопрос.*

Что составляет основу политики безопасности?

50) *Прочитайте текст и ответьте на вопрос.*

Что является первым этапом разработки системы защиты ИС?

51) *Прочитайте текст и ответьте на вопрос.*

Что являются достоинствами аппаратной реализации криптографического закрытия данных?

52) *Прочитайте текст и ответьте на вопрос.*

Что являются достоинствами программной реализации криптографического закрытия данных?

53) *Прочитайте текст и ответьте на вопрос.*

Что являются аспектами адекватности средств защиты?

54) *Прочитайте текст и ответьте на вопрос.*

Что включает процесс анализа рисков при разработке системы защиты ИС?

55) *Прочитайте текст и ответьте на вопрос.*

Что различает модели воздействия программных закладок на компьютеры?

Составил преподаватель _Скряго О.С.