СОГЛАСОВАНО
Начальник отдела защиты информации
Департамента цифрового развития
Смоленской области
_____ А.Н. Калугин
«31» 08 2020 г.

УТВЕРЖДАЮ
Заместитель директора по
учебной работе
_____ И. В. Иванешко
«31» 08 2020 г.

РАССМОТРЕНО
на заседании методической
комиссии дисциплин
средств подвижной связи
Председатель _____ Е.Н. Кожекина
Протокол №1 31.08 2020 г.

СМОЛЕНСК
ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 009533997B26BB162CCCB9A17C8FD30591
Владелец: Иванешко Ирина Васильевна
Действителен: с 22.05.2023 до 14.08.2024

Контрольно-оценочные средства для промежуточной аттестации
МДК 03.02 Технология применения комплексной системы защиты информации
ПМ.03 Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи
по специальности 11.02.09. Многоканальные телекоммуникационные системы

Дифференцированный зачет является промежуточной формой контроля, подводит итог освоения МДК 03.02.

В результате освоения МДК 03.02 студент должен освоить следующие профессиональные компетенции:

Код	Наименование профессиональных компетенций
ПК 3.1	Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.
ПК 3.2	Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.
ПК 3.3	Обеспечивать безопасное администрирование многоканальных телекоммуникационных систем и информационно-коммуникационных сетей связи.

А также общие компетенции:

Код	Наименование общих компетенций
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Иметь практический опыт:

ПО 2 – определения необходимых средств защиты;

ПО 3 – проведения аттестации объекта защиты (проверки уровня защищенности);

ПО 5 - установки, настройки специализированного оборудования по защите информации;

ПО 6 - выявления возможных атак на автоматизированные системы;

ПО 7 - установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;

ПО 8 - конфигурирования автоматизированных систем и информационно-коммуникационных сетей;

ПО 9 - проверки защищенности автоматизированных систем и информационно-коммуникационных сетей;

ПО 10 - защиты баз данных;

ПО 11 - организации защиты в различных операционных системах и средах;

ПО 12 - шифрования информации;

ПО14 – использования системы обнаружения вторжений с применением систем мониторинга;

ПО15 – использования систем защиты от распределённых атак на АИС;

ПО16 - установки, настройки специализированного программного обеспечения (свободно распространяемого программного обеспечения) по защите информации в сетях мобильной связи.

Уметь:

У2 – проводить выбор средств защиты в соответствии с выявленными угрозами;

У4 - осуществлять мероприятия по проведению аттестационных работ;

У6 - использовать программные продукты, выявляющие недостатки систем защиты;

У7 - выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;

У8 - производить установку и настройку средств защиты;

У9 - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

У10 - выполнять тестирование систем с целью определения уровня защищенности;

У11 - использовать программные продукты для защиты баз данных;

У12 - применять криптографические методы защиты информации;

У14 – использовать решения на основе технологии NAC;

У15 – использовать программно-аппаратные комплексы с применением технологий IPS (IDS).

Знать:

З2 – назначение, классификацию и принципы работы специализированного оборудования;

З3 - принципы построения информационно-коммуникационных сетей;

З4 - возможные способы несанкционированного доступа;

З8 – технологии применения программных продуктов;

З9 – возможные способы, места установки и настройки программных продуктов;

З10 - конфигурации защищаемых сетей;

З11 - алгоритмы работы тестовых программ;

З12 - средства защиты различных операционных систем и сред;

З13 - способы и методы шифрования информации;

З15 – принципы детектирования предфродового состояния;

З16 – принципы обеспечения информационной безопасности в VoIP сетях;

З17 - угрозы информационной безопасности, актуальные для виртуальных сред.

Дифференцированный зачет по МДК 03.02 проводится в форме тестирования. Тест содержит 20 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока (первый блок 160 вопросов, второй блок 150 вопросов) заданий по 10 вопросов.

Время тестирования – 90 минут (по 3 минуты на каждый вопрос тестовых позиций и по 4 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 20 минут.

Критерии оценивания:

- оценка «отлично» выставляется обучающемуся, если процент результативности (в % выполнения) составляет 90-100%;

- оценка «хорошо» «4» - ставится в том случае, если верные ответы составляют 71 -89% от общего количества;

- оценке «удовлетворительно» соответствует работа, содержащая 51-70% правильных ответов;

- оценке «неудовлетворительно» соответствует работа, содержащая менее 50% правильных ответов.

Блок заданий закрытого типа Формируемые ПК 3.1		
1.	Что из перечисленного всегда является уязвимостью?	1.Слабое место в системе, с использованием которого может быть осуществлена атака. 2. Ошибка в программном обеспечении. 3.Отсутствие политики безопасности. 4.Ошибка в настройках межсетевого экрана.
2.	Что понимается под атакой на информационную систему	1Любое действие, нарушающее безопасность информационной системы. 2.Действие или последовательность связанных между собой действий, использующих уязвимости данной информационной системы и приводящих к нарушению политики безопасности. 3.Использование ошибки в программном обеспечении. 4.Исключительно несанкционированный доступ в систему.
3.	Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется?	1.Мониторинг. 2.Аудит. 3.Управление ресурсами. 4.Администрирование.
4.	Из каких подсистем состоит dIDS?	1.Центральный анализирующий сервер. 2.Агенты сети. 3.Сервер сбора информации об атаке. 4.Система сбора и анализа событий, генерируемых различными типами СЗИ.
5.	Системы обнаружения атак на уровне узла (…) Дополните утверждение.	1.Осуществляют мониторинг активности одного узла в сети. 2.Осуществляют мониторинг активности всех сегментов сети. 3.Осуществляют консолидацию и хранение журналов событий от различных источников. 4.Предоставляют инструменты для анализа событий и разбора инцидентов.
6.	Системы обнаружения атак на уровне сети (…) Дополните утверждение.	1.Осуществляют мониторинг сетевого сегмента. 2.Осуществляют мониторинг активности одного узла в сети. 3.Осуществляют консолидацию и хранение журналов событий от различных источников. 4.Предоставляют инструменты для анализа событий и разбора инцидентов.
7.	Что способна выявлять SIEM система?	1.Сетевые атаки во внутреннем и внешнем периметрах. 2.Вирусные эпидемии или отдельные вирусные заражения, не удаленные вирусы, бэкдоры и трояны. 3.Попытки несанкционированного доступа к конфиденциальной информации. 4.Фрод и мошенничество. 5.Ошибки и сбои в работе информационных систем. 6.Уязвимости. 7.Ошибки конфигураций в средствах защиты и

		информационных системах. 8.Все ответы верны.
8.	На основании каких факторов выбираются полезные источники и правила корреляции SIEM систем?	1.Критичность системы (ценность, риски) и информации (обрабатываемой и хранимой). 2.Достоверность и информативность источника событий. 3.Покрытие каналов передачи информации. 4.Решение спектра задач ИТ и ИБ (обеспечение непрерывности, расследование инцидентов, соблюдение политик, предотвращение утечек информации и т. п.). 5.Все ответы верны.
9.	Сервис безопасности – это?	1.Сервис, который обеспечивает задаваемую политикой безопасность информационных систем и/или передаваемых данных. 2.Сервис, который определяет осуществление атаки. 3.Сервис, который предотвращает несанкционированный доступ к файлам и программам. 4.Сервис, который обеспечивает взаимодействие с вышестоящей организацией.
10.	Механизм безопасности – это? (выберите самое точное определение, один ответ)	1.Программное и/или аппаратное средство, которое определяет и/или предотвращает атаку. 2.Настройки межсетевого экрана. 3.Настройки программного обеспечения. 4.Аппаратура, которая предотвращает несанкционированный доступ к файлам и программам.
11.	Что из перечисленного не относится к сервисам безопасности?	1.Используемые математические алгоритмы. 2.Предотвращение несанкционированного доступа. 3.Обнаружение и документирование проникновения. 4.Выполнение аутентификации сервера.
12.	Что из перечисленного не относится к понятию «оборона в глубину»?	1.Использование нескольких взаимосвязанных между собой технологий. 2.Использование нескольких коммутаторов. 3.Использование нескольких межсетевых экранов. 4.Использование аппаратных средств разных производителей.
13.	Участниками аутентификационного процесса могут быть?	1.Пользователи. 2.Маршрутизаторы. 3.Межсетевые экраны. 4.Пароли.
14.	Сервис, который гарантирует, что информация получена из законного источника и получателем является тот, кто нужно, называется?	1.Аутентификацией. 2.Целостностью. 3.Конфиденциальностью. 4.Доступностью.
15.	Что необходимо для гарантирования выполнения сервисов безопасности?	1.Разработать политику безопасности. 2.Рассмотреть существующие нормативные требования и акты. 3.Обеспечить обучение сотрудников, ответственных за ИБ. 4.Обеспечить отсутствие посторонних лиц в организации.
16.	Выберете причины, по которым необходимо создавать «оборону в глубину»?	1.Ни один из сервисов безопасности не может гарантировать 100%-ную защиту. 2.Сбой единственного используемого сервиса безопасности не должен означать, что нарушитель получает полный доступ в систему. 3.Межсетевой экран не может быть конечной точкой VPN. 4.Межсетевой экран не может выполнять аутентификацию пользователей.

17.	Идентификация пользователя дает возможность вычислительной системе (…) Дополните утверждение.	1.Отличать одного пользователя от другого. 2.Гарантировать, что пользователь является тем, за кого он себя выдает. 3.Обеспечить корректное управление доступом. 4.Гарантировать отсутствие несанкционированного доступа.
18.	Что понимают под «обороной в глубину»?	1.Создание такой информационной инфраструктуры, в которой для минимизации отказов и проникновений используются несколько взаимосвязанных между собой технологий. 2.Создание такой информационной инфраструктуры, в которой используется несколько межсетевых экранов. 3.Создание такой сетевой топологии, в которой используются межсетевые экраны нескольких производителей. 4.Создание такой сетевой топологии, в которой используются межсетевые экраны одного производителя.
19.	Авторизация – это?	1.Сервис, который определяет права и разрешения, предоставляемые индивидууму (или процессу) и обеспечивает возможность доступа к ресурсу. 2.Подтверждение того, что информация получена из законного источника и получателем является тот, кто нужно. 3.Невозможность несанкционированной модификации информации. 4.Невозможность несанкционированного просмотра информации.
20.	Основное назначение межсетевого экрана состоит в том, чтобы (…) (выберите самое точное определение, один ответ)	1.Обеспечить полную безопасность локальной сети. 2.Защитить хосты и сети от использования существующих уязвимостей в стеке протоколов TCP/IP. 3.Обнаружить проникновение в локальную сеть. 4.Выполнить аутентификацию пользователей.
21.	Межсетевые экраны являются … (выберите самое точное определение, один ответ)	1.Специализированными программами, невозможна аппаратная реализация. 2.Специализированными аппаратными устройствами без встроенной ОС. 3.Специализированными аппаратными устройствами со встроенной ОС, только программная реализация невозможна. 4.Аппаратно-программными устройствами.
22.	Под термином «сетевой периметр» понимается?	1.Все компьютеры расположены в одном помещении. 2.Локальная сеть имеет четкие границы, т.е. про любой хост можно сказать, находится ли он в локальной сети или нет. 3.Все компьютеры расположены за одним маршрутизатором. 4.Вход в помещение, в котором расположены компьютеры, охраняется.
23.	При использовании межсетевого экрана предполагается, что (…)? Дополните утверждение.	1.Атаки всегда начинаются с компьютеров, расположенных за пределами сетевого периметра. 2.Атаки могут начинаться как с компьютеров, расположенных за пределами сетевого периметра, так и с компьютеров, расположенных в локальной сети. 3.Атаки всегда начинаются с компьютеров, которые не доступны с данного межсетевого экрана. 4.Атаки всегда начинаются с компьютеров, расположенных в другом помещении.
24.	К требованиям, которые накладывает	1.Используемые транспортные протоколы (IPv4 или

	внешнее окружение на функционирование межсетевого экрана, относятся?	IPv6). 2.Количество отделов в организации. 3.Специфика защищаемых сервисов. 4.Количество комнат в помещении.
25.	Политиками по умолчанию для межсетевого экрана считаются?	1.Запретить весь входящий трафик, который явно не разрешен. 2.Разрешить весь входящий трафик, который явно не запрещен. 3.Разрешить весь исходящий трафик, который явно не запрещен. 4.Запретить весь исходящий трафик, который явно не разрешен.
26.	Какой антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы?	1.Детектор. 2.Доктор. 3.Сканер. 4.Ревизор. 5.Сторож.
27.	Какой антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным?	1.Детектор. 2.Доктор. 3.Сканер. 4.Ревизор. 5.Сторож.
28.	Какие вирусы активизируются в самом начале работы с операционной системой?	1.Троянцы. 2.Загрузочные вирусы. 3.Черви.
29.	Межсетевого экрана какого класса не существует?	1.Экранирующий маршрутизатор. 2.Экранирующий коммутатор. 3.Экранирующий транспорт. 4.Экранирующий шлюз.
30.	Какую аутентификацию рекомендуется использовать при удаленном доступе?	1.Однофакторную. 2.Двухфакторную. 3.Трехфакторную.
31.	Какие записи должны вестись при аудите?	1.Вход/выход пользователей. 2.Неудачные попытки входа. 3.Все системные события 4.Зависит от уровня аудита.
32.	Каковы преимущества частных сетей?	1.Иинформация сохраняется в секрете. 2.Удаленные сайты могут осуществлять обмен информацией незамедлительно. 3.Удаленные пользователи не ощущают себя изолированными от системы, к которой они осуществляют доступ. 4.Низкая стоимость.
33.	Приложение, которое хочет предоставлять сервис, доступный по сети другим приложениям, называется?	1.Клиентом. 2.Коммутатором. 3.Маршрутизатором. 4.Сервером.
34.	Охарактеризуйте VPN?	1.Трафик шифруется для обеспечения защиты от прослушивания. 2.Трафик не шифруется для обеспечения защиты от прослушивания. 3.Осуществляется аутентификация удаленного сайта. 4.Виртуальные частные сети обеспечивают поддержку множества протоколов.
35.	Тип межсетевого экрана определяется?	1.Уровнем модели OSI, заголовки которого он анализирует. 2.ОС, на которой установлен межсетевой экран.

		3.Объемом оперативной памяти межсетевого экрана. 4.Производительностью межсетевого экрана.
36.	Выберите правильные утверждения:	1.Любой межсетевой экран может анализировать только один уровень модели OSI. 2.Любой межсетевой экран может анализировать только транспортный уровень модели OSI. 3.Большинство межсетевых экранов может анализировать несколько уровней модели OSI. 4.Любой межсетевой экран может анализировать только прикладной уровень модели OSI.
37.	Выберите правильные утверждения:	1.Межсетевые экраны могут функционировать как VPN-шлюзы. 2.Межсетевые экраны могут выполнять трансляцию адресов. 3.Межсетевые экраны могут выполнять Java-код, который передается в HTML-странице. 4.Межсетевые экраны могут выполнять маршрутизацию почтовых сообщений.
38.	Каковы преимущества пакетных фильтров?	1.Пакетный фильтр анализирует активное содержимое на прикладном уровне. 2.В логах пакетного фильтра может содержаться информация о пользователе. 3.Пакетный фильтр прозрачен для клиентов и серверов, так как не разрывает TCP-соединение. 4.Скорость.
39.	Каковы недостатки пакетных фильтров?	1.Не могут предотвратить атаки, которые используют уязвимости, специфичные для приложения. 2.В логах пакетного фильтра содержится информация только о параметрах сетевого и транспортного уровней. 3.Обычно уязвимы для атак, которые используют такие уязвимости TCP/IP, как подделка (spoofing) сетевого адреса. 4.Обычно более медленные по сравнению с прокси прикладного уровня. 5.Необходимо модифицировать ПО сервера. 6.Необходимо модифицировать ПО клиента.
40.	Выберете верные утверждения относительно VPN:	1.Осуществляется аутентификация удаленного сайта 2.Виртуальные частные сети обеспечивают поддержку множества протоколов 3.Соединение обеспечивает связь только между двумя конкретными абонентами 4.Все утверждения верны.
41.	Что такое пользовательские VPN?	1.Построены между отдельной пользовательской системой и узлом или сетью организации. 2.Используются частными пользователями для связи друг с другом. 3.Одно из названий VPN.
42.	Как осуществляется доступ к внутренней сети пользователем, подключенным через VPN?	1.Нужно просто знать адрес сервера VPN. 2.Необходимо пройти процедуру аутентификации на сервере. 3.Доступ к внутренней сети не может быть получен ни каким образом.
43.	В чем заключается суть многофакторной аутентификации?	1.Аутентифицируемой стороне необходимо предоставить несколько параметров, чтобы установить требуемый уровень доверия. 2.Аутентификация не может выполняться с помощью пароля. 3.Аутентификация должна выполняться третьей доверенной стороной.

		4.Аутентификация должна выполняться с использованием смарт-карты.
44.	Какие преимущества имеет централизованное управление идентификационными и аутентификационными данными?	1.Возможность использования многофакторной аутентификации. 2.Возможность использования цифровых подписей. 3.Легкое администрирование. 4.Возможность использования третьей доверенной стороны.
45.	В чем заключается суть управления доступом или авторизации?	1.Определение прав и разрешений пользователей по доступу к ресурсам. 2.Гарантирование того, что пользователь является тем, за кого он себя выдает. 3.Гарантирование того, что пользователь обращается к требуемому ресурсу (серверу). 4.Невозможность несанкционированного просмотра и изменения данных.
46.	Выберете основные компоненты управления доступом:	1.Субъекты. 2.Маршрутизаторы. 3.Объекты или ресурсы. 4.Разрешения (привилегии).
47.	Политика безопасности – это … (выберите самое точное определение, один ответ)	1.Совокупность административных мер, которые определяют порядок прохода в компьютерные классы. 2.Множество критериев для предоставления сервисов безопасности. 3.Совокупность как административных мер, так и множества критериев для предоставления сервисов безопасности. 4.Межсетевые экраны, используемые в организации.
48.	При разработке политики безопасности *главное*, что должен определить собственник информационных активов? (один ответ)	1.Информационные ценности, безопасность которых следует обеспечивать. 2.Атаки, которые возможны на информационные ценности. 3.Множество файлов, доступ к которым должен быть запрещен. 4.Множество сервисов, которые не должны быть доступны посторонним.
49.	Какие понятия не определяют полностью политику безопасности?	1.Множество коммутаторов и межсетевых экранов, используемых в организации. 2.Совокупность как административных мер, так и множества критериев для предоставления сервисов безопасности. 3.Административные меры, определяющие порядок доступа в помещение. 4.Административные меры, определяющие порядок доступа к рабочим станциям и серверам.
50.	При управлении доступом на уровне файловой системы для разграничения доступа используются?	1.Правила фильтрования межсетевого экрана. 2.Списки управления доступом (Access Control List – ACL). 3.БД политик безопасности. 4.Статические маршруты.
Блок заданий закрытого типа Формируемые ПК 3.2		
1.	Какие функции НЕ выполняет антивирусная защита?	1.Поиск и уничтожение известных вирусов. 2.Поиск и уничтожение неизвестных вирусов. 3.Определения адреса отправителя вирусов.
2.	Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к	1.Аутентификация. 2.Идентификация 3.Аудит 4.Авторизация

	ресурсам системы – это?	
3.	Программный модуль, который имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа?	1.Имитатор 2.Перехватчик 3.Заместитель 4.Фильтр
4.	При полномочной политике безопасности совокупность меток с одинаковыми значениями образует?	1.Уровень безопасности. 2.Область равной критичности. 3.Область равного доступа. 4.Уровень доступности.
5.	В системах управления доступом субъектом может быть?	1.Пользователь. 2.Аппаратное устройство. 3.Процесс ОС. 4.Прикладная система. 5.Все ответы верны.
6.	Что такое идентификация?	1.Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации 2.Указание на правильность выполненных операций по защите информации. 3.Определение файлов, которые изменены в информационной системе несанкционированно. 4.Выполнение процедуры засекречивания файлов. 5.Процесс периодического копирования информации.
7.	Какие меры позволяют повысить надежность парольной защиты?	1.Наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.). 2.Управление сроком действия паролей, их периодическая смена. 3.Ограничение доступа к файлу паролей. 4.Ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы"). 5.Обучение пользователей. 6.Выбор простого пароля (имя подруги, название спортивной команды).
8.	Что относится к идентификации и/или аутентификации людей на основе их физиологических характеристик?	1.Анализ особенностей голоса. 2.Распознавание речи; 3.Отпечатки пальцев; 4.Сканирование радужной оболочки глаза; 5.Анализ знаний по информационной безопасности. 6.Анализ динамики подписи (ручной).
9.	Что относится к идентификации и/или аутентификации людей на основе их поведенческих характеристик?	1.Анализ динамики подписи (ручной). 2.Анализ стиля работы с клавиатурой. 3.Анализ отпечатков пальцев. 4.Анализ административных указаний по информационной безопасности. 5.Анализ тембра голоса.
10.	Назовите наиболее точные способы идентификации человека:	1.Удостоверение личности с фотографией (паспорт). 2.Отпечатки пальцев (папиллярные узоры). 3.Узор радужной оболочки или сетчатки глаза.
11.	Каковы преимущества пользовательских VPN?	1.Сотрудники, находящиеся в командировке могут подключаться к сети компании. 2.Сотрудники могут работать из дома. 3.Преимуществ нет.
12.	Сервер VPN – это?	1.Любой компьютер в сети 2.Компьютер в сети, выступающий в роли конечного узла. 3.Компьютер к которому могут подключаться

		пользователи.
13.	Что из перечисленного относится к аппаратным средствам аутентификации?	1.Электронные ключи. 2.Смарт-карты. 3.S/KEY. 4.Kerberos.
14.	Выберите из предложенных вариантов пароля "правильный" (с точки зрения современных требований к паролю):	1.1rR%56ty. 2.i23Y65. 3.mersqwertyp. 4.3488714567747865.
15.	Некоторая уникальная информация, позволяющая различать пользователей называется?	1.Идентификатор (логин). 2.Пароль. 3.Учетная запись. 4.Ключ.
16.	Секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется?	1.Идентификатор (логин). 2.Пароль. 3.Учетная запись. 4.Ключ.
17.	Совокупность идентификатора и пароля пользователя называется?	1.Логин пользователя. 2.Учетная запись пользователя. 3.Ключ пользователя.
18.	Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является?	1.Идентификацией пользователя. 2.Аутентификацией пользователя. 3.Опознанием пользователя. 4.Созданием учетной записи пользователя.
19.	Проверка принадлежности пользователю предъявленного им идентификатора является:	1.Идентификацией пользователя. 2.Аутентификацией пользователя. 3.Регистрацией пользователя. 4.Созданием учетной записи пользователя.
20.	Для чего нужна система контроля доступа?	1.Предотвратить проникновение на частную территорию посторонних лиц. 2.Организовать учет рабочего времени, фиксацию времени въезда и выезда транспортных средств. 3.Защитить материальные ценности, включая производственное и офисное оборудование, от повреждений и кражи. 4.Все ответы верны.
21.	Под DoS-атакой понимается?	1.Модификация передаваемого сообщения. 2.Повторное использование нарушителем перехваченного ранее сообщения. 3.Невозможность доступа в систему законным пользователем. 4.Невозможность получения сервиса законным пользователем.
22.	Невозможность получения сервиса законным пользователем называется?	1.DoS-атакой. 2.Replay-атакой. 3.Пассивной атакой. 4.Атакой «man-in-the-middle».
23.	Что не относится к DoS-атаке?	1. Выполнение незаконного проникновения в систему. 2.Определение топологии сети. 3.Попытка исчерпать какие-либо ресурсы на целевой системе. 4.Попытка монополизировать сетевое соединение.
24.	Какие шаги следует предпринять при обнаружении подозрительного трафика?	1.Идентифицировать системы. 2.Записывать в журнал сведения о дополнительном трафике между источником и пунктом назначения. 3.Заблокировать удаленную систему. 4.Записывать в журнал весь трафик, исходящий из

		источника. 5.Записывать в журнал содержимое пакетов из источника.
25.	Где лучше размещать VPN сервер?	1.В отдельной DMZ. 2.В DMZ интернета, вместе с остальными серверами. 3.Во внутренней сети компании.
26.	Какой должна быть система аутентификации, использующаяся в VPN?	1.Однофакторной. 2.Двухфакторной. 3.Трехфакторной. 4.Четырехфакторной.
27.	Атаки сканирования могут определять?	1.Топологию целевой сети. 2.Типы сетевого трафика, пропускаемые межсетевым экраном. 3.Операционные системы, которые выполняются на хостах. 4.ПО сервера, которое выполняется на хостах. 5.Номера версий для всего обнаруженного ПО. 6.Все ответы верны.
28.	Какое средство аутентификации рекомендуется использовать в VPN?	1.Смарт-карту и пароль. 2.Только смарт-карту. 3.Только пароль. 4.Биометрическую идентификацию.
29.	Атака IP Spoofing состоит в том, что …?	1.Нарушитель изменяет IP-адрес получателя на IP-адрес доверенного хоста. 2.Нарушитель изменяет содержимое протокола прикладного уровня. 3. Нарушитель изменяет IP-адрес источника на IP-адрес доверенного хоста. 4.Нарушитель изменяет номер порта получателя.
30.	Какие из указанных контрмер позволяют компенсировать физические уязвимости?	1.Межсетевые экраны. 2.Устройства считывания смарт-карт при входе в помещения. 3.Охрана. 4.Шифрование.
31.	Как должна настраиваться политика аудита?	1.В соответствии с политикой безопасности организации. 2.Так, чтобы зафиксировать все события в системе. 3.Так, чтобы фиксировался необходимый минимум событий.
32.	Наличие какого элемента характерно для всех архитектур DMZ?	1.Почтовый сервер. 2.DNS. 3.NTP. 4.Межсетевой экран.
33.	Как расшифровывается аббревиатура DMZ?	1.Демилитаризованная зона. 2.Зона управления данными. 3.Зона ежедневного управления. 4.Зона поддержки данных.
34.	В сети демилитаризованной зоны (DMZ) должны располагаться?	1.Рабочие станции пользователей. 2.Серверы, которые должны быть доступны только внутренним пользователям. 3.Серверы, которые должны быть доступны из внешних сетей. 4.Серверы, содержащие наиболее чувствительные данные.
35.	Какими свойствами обладает интерфейс на аппаратном межсетевом экране интерфейс, маркированный как dmz?	1.Этот интерфейс допускает только входящий трафик. 2.Этот интерфейс допускает только исходящий трафик. 3.К этому интерфейсу могут быть подключены только сервера. 4.Этот интерфейс может указываться в правилах

		фильтрования и для него могут быть указаны собственные маршруты.
36.	Выберите наиболее оптимальное окружение межсетевого экрана:	1.Конечные точки VPN совмещены с межсетевым экраном. 2.Конечные точки VPN расположены за межсетевым экраном. 3.Конечные точки VPN и межсетевой экран расположены в разных точках входа в локальную сеть. 4.Конечные точки VPN расположены перед межсетевым экраном.
37.	Если в организации есть веб-сервер для внешних пользователей и веб-сервер для получения информации своими сотрудниками, то оптимальным количеством DMZ является?	1.Одна DMZ. 2.Две DMZ. 3.Три DMZ. 4.Четыре DMZ.
38.	Какие из перечисленных веб-серверов следует расположить во внешней DMZ?	1.Веб-сервер, на котором осуществляется on-line'овый заказ услуг. 2.Веб-сервер, на котором публикуются распоряжения руководства организации. 3.Веб-сервер, на котором могут находиться личные данных сотрудников. 4.Веб-сервер, на котором опубликованы общедоступные телефоны и координаты организации.
39.	Как называется атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе?	1.«Отказ от обслуживания» (Denial of Service - DoS). 2.Срыв стека. 3.Внедрение на компьютер деструктивных программ. 4.Перехват передаваемой по сети информации (Sniffing). 5.Спуфинг. 6.Сканирование портов.
40.	Как называется атака, целью которой является трафик локальной сети?	1.«Отказ от обслуживания» (Denial of Service - DoS). 2.Срыв стека. 3.Внедрение на компьютер деструктивных программ. 4.Перехват передаваемой по сети информации (Sniffing). 5.Спуфинг. 6.Сканирование портов.
41.	Как называется атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой?	1.«Отказ от обслуживания» (Denial of Service - DoS). 2.Срыв стека. 3.Внедрение на компьютер деструктивных программ. 4.Перехват передаваемой по сети информации (Sniffing). 5.Спуфинг. 6.Сканирование портов.
42.	Как называется сетевая атака, целью которой является поиск открытых портов работающих в сети устройств, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих устройствах?	1.«Отказ от обслуживания» (Denial of Service - DoS). 2.Срыв стека. 3.Внедрение на компьютер деструктивных программ. 4.Перехват передаваемой по сети информации (Sniffing). 5.Спуфинг. 6.Сканирование портов.
43.	Что следует определить при анализе производительности межсетевого экрана?	1.Какую пропускную способность, максимальное количество одновременно открытых соединений, соединений в секунду может обеспечивать межсетевой экран. 2.Возможна ли балансировка нагрузки и резервирование для гарантирования высокой отказоустойчивости.

		3.Что является более предпочтительным – аппаратный или программный межсетевой экран. 4.Какое количество портов существует на выбранном экземпляре межсетевого экрана.
44.	Что следует рассмотреть при внедрении персональных межсетевых экранов и межсетевых экранов для хостов?	1.Удовлетворяют ли рабочие станции и сервера минимальным системным требованиям, которые необходимы для функционирования межсетевого экрана. 2.Будет ли межсетевой экран совместим с другим ПО обеспечения безопасности на рабочей станции или сервере (например, с ПО обнаружения вредоносного кода). 3.Возможно ли централизованное управление межсетевым экраном, и могут ли политики, которые обеспечивают безопасность организации, автоматически загружаться на клиентские машины. 4.Необходимо ли изменить пароль администратора на рабочей станции.
45.	При использовании IDS (…) Дополните утверждение.	1.Возрастает возможность определения преамбулы атаки. 2.Возрастает возможность фильтрования трафика. 3.Возрастает возможность определения оптимального маршрута для каждого кадра. 4.Возрастает возможность раскрытия осуществленной атаки.
46.	IDS могут быть реализованы (…) Дополните утверждение.	1.Только программно. 2.Только аппаратно. 3.Только совместно с межсетевым экраном. 4.Как программно, так и аппаратно.
47.	Каковы преимущества использования IDS?	1.Возможность иметь реакцию на атаку. 2.Возможность блокирования атаки. 3.Выполнение документирования существующих угроз для сети и систем. 4.Нет необходимости в межсетевых экранах.
48.	Что следует учитывать при выборе IDS?	1.Ценность защищаемых информационных ресурсов. 2.Количество пользовательских аккаунтов в локальной сети. 3.Количество административных аккаунтов в локальной сети. 4.Загруженность сети.
49.	Какие возможности может обеспечивать IDS?	1.Возможность определения внешних угроз. 2.Возможность шифрования трафика. 3.Возможность иметь реакцию на атаку. 4.Возможность фильтрации трафика.
50.	Что анализируется при определении злоупотреблений?	1.Анализируются события на соответствие некоторым образцам, называемым «сигнатурами атак». 2.Анализируются события для обнаружения неожиданного поведения. 3.Анализируются подписи в сертификатах открытого ключа. 4.Анализируется частота возникновения некоторого события.
51.	Что анализируется при определении аномалий?	1.Анализируется частота возникновения некоторого события. 2.Анализируются различные статистические и эвристические метрики. 3.Анализируются события на соответствие некоторым образцам, называемым «сигнатурами атак». 4.Анализируется исключительно интенсивность

		трафика.
52.	Для чего используются системы анализа уязвимостей?	1.Для создания «моментального снимка» состояния безопасности системы. 2.Как альтернатива IDS, полностью заменяя ее. 3.Как альтернатива политики безопасности предприятия, являясь полным ее аналогом. 4.Как альтернатива межсетевым экранам, полностью заменяя их.
53.	На основании чего осуществляется управление доступом в пакетном фильтре?	1.IP-адреса источника. 2.IP-адреса назначения. 3.Номера привила в наборе правил пакетного фильтра. 4.Учетной записи и пароля пользователя.
54.	Выберите правильное утверждение:	1. Администрирование межсетевого экрана должно осуществляться только через интерфейс командной строки. 2.Администрирование межсетевого экрана должно осуществляться только через графический интерфейс пользователя. 3.Администрирование межсетевого экрана должно осуществляться с использованием собственного протокола доступа. 4.Администрирование межсетевого экрана может осуществляться как через интерфейс командной строки, так и через графический интерфейс пользователя.
55.	Какими возможностями должны обладать межсетевые экраны для фильтрования IPv6?	1.Если межсетевой экран используется для запрещения прохождения IPv6-трафика в сеть, то он может не распознавать туннелированный v6-to-v4 трафик. 2.Межсетевой экран должен пропускать трафик v6-to-v4, даже если политика безопасности запрещает IPv6-трафику проходить в сеть. 3. Если межсетевой экран используется для запрещения прохождения IPv6-трафика в сеть, то он должен распознавать и блокировать все формы v6-to-v4 туннелирования. 4.Межсетевой экран должен запрещать трафик v6-to-v4, даже если политика безопасности разрешает IPv6-трафику проходить в сеть.
56.	Межсетевые экраны, расположенные на границе сетевого периметра (…) Дополните утверждение.	1.Должны запрещать весь входящий и исходящий ICMP-трафик, за исключением отдельных типов и кодов, которые должны быть специально разрешены. 2.Должны запрещать весь входящий ICMP-трафик. 3.Должны запрещать весь исходящий ICMP-трафик. 4.Весь ICMP-трафик должен быть всегда разрешен.
57.	Трансляция сетевых адресов (NAT) позволяет (…) Дополните утверждение.	1.Скрыть логины пользователей локальной сети. 2.Скрыть пароли пользователей локальной сети. 3.Скрыть сетевой адрес самого межсетевого экрана. 4.Скрыть схему сетевой адресации локальной сети.
58.	NAT используется (…) Дополните утверждение.	1.В IPv4. 2.В IPv6. 3.В IPv32. 4.В IPv64.
59.	Где располагается маршрутизатор NAT?	1.Расположен на границе между двумя областями адресов и преобразует адреса в IP-заголовках таким образом, что пакет корректно маршрутизируется при переходе из одной области в другую. 2.Расположен на границе между двумя областями адресов, в одной из которых адреса принадлежат частной сети, а в другой – внешней. 3.Расположен на границе между локальной сетью и

		интернетом. 4.Расположен на границе между двумя локальными сетями с разными требованиями к безопасности.
60.	Для каких целей устанавливается IDS?	1.Обнаружение атак 2.Предотвращение атак 3.Обнаружение нарушений политики 4.Повышение надежности системы.
Блок заданий закрытого типа Формируемые ПК 3.3		
1.	Что из перечисленного понимается под безопасностью информационной системы?	1.Защита от неавторизованного доступа или модификации информации во время хранения, обработки или пересылки. 2.Защита от отказа в обслуживании законных пользователей. 3.Меры, необходимые для определения, документирования и учета угроз. 4.Отсутствие выхода в интернет.
2.	Какие устройства могут выполнять функции NAT?	1.Маршрутизаторы. 2.Межсетевые экраны. 3.Почтовые сервера. 4.DNS сервера.
3.	В системах управления доступом *объектом доступа* может быть?	1.Файл. 2.Любой сетевой ресурс, к которому субъект хочет получить доступ. 3.Аппаратное устройство. 4.Прикладная система. 5.Все ответы верны.
4.	При управлении доступом на сетевом уровне для разграничения трафика используются?	1.Маршрутизаторы. 2.Межсетевые экраны. 3.Коммутаторы. 4.Веб-сервера.
5.	На основании чего осуществляется управление доступом в пакетном фильтре?	1.Типа трафика. 2.Порта источника. 3.Номера привила в наборе правил пакетного фильтра. 4.Порта назначения.
6.	Технология VLAN не позволяет … Дополните утверждение.	1.Выполнять шифрование трафика. 2.Выполнять фильтрование пакетов, основываясь на правилах. 3.Выполнять аутентификацию на уровне пользователя. 4.Предотвратить широковещательные штормы.
7.	Технология VLAN позволяет … Дополните утверждение.	1.Исключить передачу кадров между разными виртуальными сетями независимо от типа IP-адреса – уникального, группового или широковещательного. 2.Выполнять фильтрование пакетов, основываясь на правилах, указанных при создании VLAN. 3.Выполнять аутентификацию пользователей. 4.Выполнять шифрование трафика.
8.	Какие типы аппаратных устройств могут поддерживать технологию VLAN?	1.Концентраторы. 2.Коммутаторы. 3.Межсетевые экраны. 4.Веб-серверы.
9.	Виртуальной локальной сетью (vlan) называется?	1.Логическая группа хостов в сети, трафик которой, в том числе и широковещательный, полностью изолирован на канальном уровне от хостов из других виртуальных локальных сетей. 2.Логическая группа хостов в сети, трафик которой полностью изолирован на сетевом уровне от хостов из других виртуальных локальных сетей. 3.Логическая группа хостов в сети, трафик которой

		полностью изолирован на прикладном уровне от хостов из других виртуальных локальных сетей. 4.Логическая группа хостов в сети, трафик которой аутентифицируется межсетевым экраном.
10.	Использование технологии VLAN позволяет (…) Дополните утверждение.	1.На межсетевом экране указывать параметры шифрования трафика, не используя протоколы туннелирования. 2.На межсетевом экране создавать политики, которые управляют доступом друг к другу хостов из разных VLAN. 3.Выполнить аутентификации трафика. 4.Обеспечить целостность трафика.
11.	При использовании технологии VLAN повышается безопасность, так как (…) Дополните утверждение.	1.Трафик, проходящий по VLAN, зашифрован. 2.Трафик, проходящий по VLAN, аутентифицирован. 3.Трафик, проходящий по VLAN, может фильтроваться правилами межсетевого экрана. 4.Для трафика, проходящего по VLAN, обеспечивается целостность.
12.	Межсетевые экраны прикладного уровня могут (…) Дополните утверждение.	1.Выполнять аутентификацию пользователя. 2.Автоматически распознавать новые протоколы. 3.Шифровать данные пользователя. 4.Выполнять авторизацию пользователя.
13.	Межсетевые экраны прикладного уровня не могут (…) Дополните утверждение.	1.Выполнять аутентификацию пользователя. 2.Автоматически распознавать новые протоколы. 3.Шифровать данные пользователя. 4.Выполнять авторизацию пользователя.
14.	Межсетевые экраны прикладного уровня (…) Дополните утверждение.	1.Должны иметь агента для каждого уровня модели OSI. 2.Могут быть реализованы исключительно программно. 3.Анализируют содержимое прикладного уровня. 4.Должны иметь агента для каждого прикладного протокола.
15.	Выделенные прокси-серверы предназначены для того, чтобы обрабатывать трафик (какой?) Дополните утверждение.	1.Конкретного уровня модели OSI. 2.Конкретного прикладного протокола. 3.Конкретного адреса отправителя. 4.Конкретного пользователя.
16.	Выберете недостаток межсетевых экранов прикладного уровня:	1.Производительность межсетевого экрана прикладного уровня ниже, чем у пакетного фильтра. 2.Межсетевой экран прикладного уровня обязательно разрывает TCP-соединение. 3.Межсетевой экран прикладного уровня не может анализировать заголовки транспортного и сетевого уровней. 4.Межсетевой экран прикладного уровня обеспечивает меньший уровень безопасности, чем пакетный фильтр.
17.	Прокси-шлюзы прикладного уровня (выберите самое точное определение, один ответ)	1.Имеют прокси-агента, являющегося посредником между клиентом и сервером. 2.Имеют базу данных пользователей, которым разрешен доступ к защищаемому ресурсу. 3.Не разрывают TCP-соединение. 4.Имеют базу данных IP-адресов, с которых разрешен доступ к защищаемому ресурсу.
18.	При использовании прокси-шлюзов прикладного уровня (…) Дополните утверждение.	1.Внутренние IP-адреса не видны вовне. 2.Внешние IP-адреса не видны изнутри. 3.Прокси-шлюз является абсолютно прозрачным для клиента. 4.Прокси-шлюз изменяет IP-адрес источника на свой IP-адрес.
19.	Что определяет процедура управления	1.Кто может осуществлять авторизованный доступ к тем

	пользователями?	или иным компьютерам организации, и какую информацию администраторы должны предоставлять пользователям, запрашивающим поддержку. 2.Каким образом в данный момент времени применяется политика безопасности на различных системах, имеющихся в организации 3.Шаги по внесению изменений в функционирующие системы.
20.	Каковы общие свойства систем анализа уязвимостей и систем обнаружения вторжений?	1.И те, и другие следят за конкретными симптомами проникновения и другими нарушениями политики безопасности. 2.И те, и другие могут фильтровать трафик. 3.И те, и другие могут шифровать трафик. 4.И те, и другие могут аутентифицировать пользователей.
21.	Что предполагает гарантирование доступности?	1.Определение точек возможного сбоя и ликвидация этих точек. 2.Определение критически важных устройств. 3.Определение критически важных сервисов. 4.Определение списков управления доступом.
22.	Что необходимо обеспечить при управлении конфигурациями?	1.Регулярное изменение правил фильтрации. 2.Регулярное обновление ПО. 3.Управление изменениями. 4.Оценка состояния сетевой безопасности.
23.	Традиционный (или исходящий) NAT (…) Дополните утверждение.	1.Обеспечивает конфиденциальность трафика между клиентами, расположенными во внешней сети, и серверами, расположенными в частной сети. 2.Обеспечивает конфиденциальность трафика между клиентами, расположенными в частной сети, и серверами, расположенными во внешней сети. 3.Позволяет хостам во внешней сети прозрачно получать доступ к хостам в частной сети. 4. Позволяет хостам в частной сети прозрачно получать доступ к хостам во внешней сети.
24.	Для каких целей необходимо использование третьей доверенной стороны?	1.Создания зашифрованных туннелей. 2.Изменения правил фильтрования трафика. 3.Распределения между двумя участниками секретной информации, которая не стала бы доступна оппоненту.
25.	Что из перечисленного относится к механизмам безопасности?	1.Хэш-функции. 2.Целостность сообщения. 3.Алгоритмы симметричного шифрования. 4.Аутентификация сообщения.
26.	Что из перечисленного не относится к механизмам безопасности?	1.Хэш-функции. 2.Целостность сообщения. 3.Алгоритмы симметричного шифрования. 4.Аутентификация сообщения.
27.	Межсетевые экраны с поддержкой состояния являются пакетными фильтрами, которые (…) Дополните утверждение.	1.Анализируют логин и пароль пользователя. 2.Анализируют транспортный уровень модели OSI. 3.Анализируют сетевой уровень модели OSI 4.Анализируют прикладной уровень модели OSI.
28.	К каким серьезным негативным последствиям может привести некорректная работа или незапланированный простой системы информационной безопасности?	1.Нарушение функционирования ИТ-инфраструктуры. 2.Остановка рабочего процесса. 3.Нарушение конфиденциальности, целостности или доступности служебной информации. 4.Отсутствие квалифицированного технического обслуживания.
29.	Под унифицированным управлением угрозами (Unified Threat Management – UTM) понимают?	1.Централизованное управление несколькими сетевыми устройствами. 2.Создание базы данных потенциальных угроз.

		3.Создание базы данных точек входа в сеть. 4.Централизованное управление всеми межсетевыми экранами.
30.	Что следует определить при анализе назначения межсетевого экрана?	1.Какие типы трафика должны защищаться. 2.Какие типы технологий межсетевых экранов лучше всего подходят для трафика, который должен быть защищен. 3.Какие дополнительные возможности безопасности – такие как возможности обнаружения проникновения, VPN, фильтрование содержимого – должен поддерживать межсетевой экран. 4.Какие способы управления поддерживает данный межсетевой экран.
31.	Что включает в себя типичная система унифицированного управления угрозами?	1.Межсетевой экран с возможностями определения и удаления вредоносного ПО на находящихся под его управлением хостах. 2.Межсетевой экран с возможностями блокирования нежелательного трафика. 3.Рабочие станции пользователей. 4.Сервера, предоставляющие сервисы удаленным пользователям.
32.	Каковы преимущества использования системы унифицированного управления угрозами?	1.Увеличивается пропускная способность сети. 2.Уменьшается сложность управления. 3.Увеличивается безопасность сетевого периметра. 4.Уменьшается количество попыток несанкционированного доступа.
33.	Для каких систем пригодна статическая NAT?	1.Для любых систем. 2.Для систем в DMZ. 3.Для клиентских рабочих станций.
34.	Что обеспечивает канальный уровень модели OSI?	1.Выполняет аутентификацию пользователя. 2.Маршрутизирует пакеты между локальными сетями. 3.Обеспечивает проверку и коррекцию ошибок. 4.Упаковывает данные в стандартные кадры для передачи через физический уровень.
35.	Что обеспечивает сетевой уровень модели OSI?	1.Обеспечивает надежность соединения. 2.Обеспечивает целостность соединения. 3.Обеспечивает конфиденциальность соединения. 4.Маршрутизирует пакеты между локальными сетями.
36.	Что обеспечивает транспортный уровень модели OSI?	1.Все протоколы данного уровня гарантируют надежность соединения. 2.Предоставляет сервисы, ориентированные на соединение. 3.Некоторые протоколы данного уровня обеспечивают целостность соединения. 4.Некоторые протоколы данного уровня гарантируют надежность соединения.
37.	Где устанавливают межсетевые экраны для веб-приложений?	1.Перед защищаемым веб-сервером (трафик вначале передается межсетевому экрану, затем веб-серверу). 2.После защищаемого веб-сервера (трафик вначале передается веб-серверу, затем межсетевому экрану). 3.Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, трафик между ними запрещен. 4.Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, но трафик между ними не запрещен.
38.	Как должны функционировать межсетевые экраны для веб-приложений?	1.Должны всегда сами выполнять аутентификацию пользователей. 2.Должны реализовывать те же функциональные

		возможности, что и защищаемый ими веб-сервер. 3.Должны одновременно являться и конечными точками VPN. 4.Должны понимать все особенности протокола HTTP.
39.	Почему существует необходимость в межсетевых экранах для виртуальных инфраструктур?	1.Сетевой трафик, который передается между гостевыми ОС внутри хоста, не может просматриваться внешним межсетевым экраном. 2.Сетевой трафик, который передается между гостевыми ОС внутри хоста, передается в зашифрованном виде. 3.Сетевой трафик, который передается между гостевыми ОС внутри хоста, использует протоколы, отличные от TCP/IP. 4.В сетевом трафике, который передается между гостевыми ОС внутри хоста, указаны другие номера портов, чем в обычном сетевом трафике.
40.	Какие особенности имеет межсетевой экран на основе приложения?	1.Управление доступом основано на запуске приложений или сервисов, а не на доступе к портам или сервисам. 2.Управление доступом основано на аутентификационных данных пользователя. 3.Управление доступом основано на сетевой активности пользователя. 4.Управление доступом основано на параметрах безопасности, указанных на шлюзе по умолчанию.
41.	В чем заключается ограниченность анализа межсетевого экрана?	1.Не может анализировать зашифрованные прикладные данные. 2.Не может выполнять аутентификацию пользователя. 3.Не может анализировать данные прикладного уровня. 4.Не может отбрасывать пакеты.
42.	Что определяет политика межсетевого экрана?	1.Как межсетевой экран будет обрабатывать сетевой трафик для определенных IP-адресов и диапазонов адресов, протоколов, приложений и типов содержимого. 2.Как межсетевой экран будет маршрутизировать пакеты. 3.Как межсетевой экран будет обеспечивать качество обслуживания (QoS). 4.Как межсетевой экран будет обеспечивать балансировку нагрузки.
43.	Что следует определить перед разработкой политики межсетевого экранирования?	1.Определить типы трафика, которые необходимы организации. 2.Определить VPN-интерфейсы, через которые должен проходить трафик. 3.Определить vlan-интерфейсы, через которые должен проходить трафик. 4.Определить статическую маршрутизацию для различных типов трафика.
44.	Как должно *всегда* выполняться администрирование межсетевого экрана? Выберете правильные ответы.	1.По защищенному каналу. 2.Из Интернет – по защищенному каналу и с использованием строгой аутентификации. 3.Из локальной сети возможно администрирование без выполнения строгой аутентификации. 4.С использованием строгой аутентификации.
45.	Для каких систем пригодна динамическая NAT?	1.Для любых систем. 2.Для систем в DMZ. 3.Для клиентских рабочих станций.
46.	Как называется способ реализации криптографического метода, при котором все процедуры шифрования и расшифрования выполняются	1.Аппаратный. 2.Программный. 3.Ручной. 4.Электромеханический.

	специальными электронными схемами по определенным логическим правилам?	
47.	Что общего имеют все методы шифрования с закрытым ключом?	1.В них для шифрования информации используется один ключ, а для расшифрования – другой ключ. 2.В них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов. 3.В них производится сложение символов исходного текста и ключа по модулю, равному числу букв в алфавите. 4.В них для шифрования и расшифрования информации используется один и тот же ключ.
48.	Где можно получить самые последние антивирусные базы?	1.На сайте компании-производителя используемой антивирусной программы. 2.Они поставляются одновременно с дистрибутивом антивирусной программы. 3.На сайте Европейского института компьютерных антивирусных исследований. 4.На сайте www.eicar.org.
49.	Какой способ внешнего доступа к внутренним системам наиболее распространен?	1.VPN. 2.Коммутируемое соединение 3.Telnet 4.Арендуемый канал.
50.	Сколько интерфейсов у межсетевого экрана прикладного уровня?	1.Один. 2.Два. 3.По одному на каждую сеть, к которым он подключен.

Блок заданий открытого типа
Формируемые ПК 3.1.

1.Процедура распознавания субъекта в процессе регистрации в системе называется?
2.Процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует, называется?
3.Процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации называется?
4.Технология идентификации, основанная на использовании радиочастотного электромагнитного излучения, называется?
5.Технология беспроводной высокочастотной связи малого радиуса действия (до 10 см), позволяющая осуществлять бесконтактный обмен данными между устройствами, расположенными на небольших расстояниях, называется?
6.Наносимая в виде штрихов закодированная информация о некоторых наиболее существенных параметрах объекта, считываемая при помощи специальных устройств, называется?
7.Двумерный штрихкод, в котором кодируется информация, состоящая из символов (включая кириллицу, цифры и спецсимволы), называется?
8.Идентификация человека по уникальным биологическим признакам называется?
9.На какие две группы делятся методы биометрической идентификации?
10.Какие методы биометрической идентификации основываются на уникальной физиологической характеристике человека, данной ему от рождения и неотъемлемой от него?
11.В основе какого метода биометрической идентификации используется уникальный для каждого человека рисунок паппилярных узоров на пальцах, т.е. отпечаток, полученный с помощью специального сканера, который преобразуется в цифровой код (свертку), и сравнивается с ранее введенным эталоном?

12.Какой метод биометрической идентификации построен на геометрии кисти руки, когда с

помощью специального устройства, состоящего из камеры и нескольких подсвечивающих диодов (включаясь по очереди, они дают разные проекции ладони), строится трехмерный образ кисти руки, по которому формируется свертка и распознается человек?
13.При каком методе биометрической идентификации с помощью инфракрасной камеры считывается рисунок вен на лицевой стороне ладони или кисти руки, полученная картинка обрабатывается, и по схеме расположения вен формируется цифровая свертка.
14.При каком способе биометрической идентификации используется рисунок кровеносных сосудов глазного дна, для того чтобы этот рисунок стал виден – человеку нужно посмотреть на удаленную световую точку, и таким образом подсвеченное глазное дно сканируется специальной камерой?
15.При каком способе биометрической идентификации достаточно портативной камеры со специализированным программным обеспечением, позволяющим захватывать изображение части лица, из которого выделяется изображение глаза и рисунок, по которому строится цифровой код для идентификации человека?
15.При каком методе биометрической идентификации строится трехмерный образ лица человека, - на лице выделяются контуры бровей, глаз, носа, губ и т.д., вычисляется расстояние между ними и строится не просто образ, а еще множество его вариантов на случаи поворота лица, наклона, изменения выражения?
16. В основе какого метода биометрической идентификации лежит уникальность распределения на лице артерий, снабжающих кровью кожу, которые выделяют тепло и используются специальные камеры инфракрасного диапазона?
17.Какие методы биометрической идентификации используются только для специализированных экспертиз, так как работают достаточно долго?
18.Какие методы биометрической идентификации основываются на поведенческой характеристике человека, построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия?
19. При каком методе биометрической идентификации не нужно никакого специального оборудования, кроме стандартной клавиатуры, - основной характеристикой, по которой строится свертка для идентификации – динамика набора кодового слова?
20.Какие системы кодируют в цифровом виде и хранят индивидуальные характеристики, позволяющие практически безошибочно идентифицировать любой индивид?
21.Метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает более эффективную защиту аккаунта, называется?
22.При каком методе идентификации пользователя первый рубеж - это логин и пароль, второй - специальный код, приходящий по SMS или электронной почте?
23.При каком способе аутентификации используются аутентификационные факторы нескольких типов.
24.Как называют пластиковые карты со встроенной микросхемой, в большинстве случаев содержащие микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти.
25.Какое компактное USB-устройство, предназначено для безопасной аутентификации пользователей, защищенного хранения ключей шифрования и ключей электронной подписи, а также цифровых сертификатов?
26.Какое USB-устройство обеспечивает двухфакторную аутентификацию в компьютерных системах и для успешной аутентификации требуется выполнение двух условий: физическое наличие самого USB-токена и знание PIN-кода к нему?
27.Какое персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживает работу с цифровыми сертификатами и электронной цифровой подписью, исполняется в виде USB-ключей, смарт-карт, комбинированных устройств и автономных генераторов одноразовых паролей?

28.При каком методе аутентификации по одноразовым паролям пользователь отправляет на

сервер свой логин; сервер генерирует некую случайную строку и посылает ее обратно; пользователь с помощью своего ключа зашифровывает эти данные и возвращает их серверу; сервер в это время «находит» в своей памяти секретный ключ данного пользователя и кодирует с его помощью исходную строку, сравнивает оба результата шифрования и при их полном совпадении считается, что аутентификация прошла успешно?

29.При каком методе аутентификации программное или аппаратное обеспечение пользователя генерирует исходные данные, которые будут зашифрованы и отправлены на сервер для сравнения (в процессе создания строки используется значение предыдущего запроса), сервер тоже обладает этими сведениями; зная имя пользователя, он находит значение предыдущего его запроса и генерирует по тому же алгоритму точно такую же строку, зашифровав ее с помощью секретного ключа пользователя (он также хранится на сервере), сервер получает значение, которое должно полностью совпадать с присланными пользователем данными?

30.При каком методе аутентификации в качестве исходной строки выступают текущие показания таймера специального устройства или компьютера, на котором работает человек, эти данные зашифровываются с помощью секретного ключа и в открытом виде отправляются на сервер вместе с именем пользователя, сервер при получении запроса на аутентификацию выполняет те же действия: получает текущее время от своего таймера и зашифровывает его; после этого сервер сравнивает два значения: вычисленное и полученное от удаленного компьютера?

31.При каком методе аутентификации в качестве исходной строки используется количество успешных процедур аутентификации, проведенных до текущей, это значение подсчитывается обеими сторонами отдельно друг от друга?

32.Совокупность технических средств, направленных на контроль входа и выхода в помещение с целью обеспечения безопасности и регулирования посещения определённого объекта, - это?

33.Какие системы автоматизируют процесс управления учетными записями, например, управляют процессом по созданию, изменению и блокированию учетных записей?

34. Какое программное решение, выступает в роли посредника между пользователем браузера и веб-сервером, и работает по принципу Man in the Middle, подменяя сертификаты пользователя и сервера?

35. Какое программное решение выступает в роли посредника между пользователем браузера и веб-сервером, и защищает внутренние веб-ресурсы организации - порталы, веб-почту?

36.Комплекс подходов, практик, технологий и специальных программных средств для управления учётными данными пользователей, с целью повышения безопасности и производительности информационных систем при одновременном снижении затрат, оптимизации времени простоя и сокращения количества повторяющихся задач, - это?

37. Метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения, - это?

38.Какая модель доступа базируется на явно заданных для каждого субъекта (пользователя) правах доступа к объектам / сегментам информации, они представляются в виде матрицы, в которой указываются полномочия субъекта относительно каждого объекта или сегмента информации?

39. Что такое ERP (Enterprise Resource Planning) система?

40.В системе управления пользователями данных, применяющей эту модель, всем субъектам (сотрудникам) и объектам (единицам информации: файлам, папкам и так далее) назначаются метки (мандаты), соответствующие разным уровням конфиденциальности. Субъект имеет право на чтение только тех объектов, уровень конфиденциальности которых не выше его уровня. Право на запись / изменение у субъекта есть при условии, что уровень конфиденциальности объекта не ниже его. Как называют эту модель доступа?

41.Какой компонент управления доступом требует от пользователей подтверждения своей личности с использованием как минимум двух или более различных факторов проверки, прежде чем получить доступ к какому-либо ресурсу?

42.Какой открытый стандарт децентрализованной системы аутентификации предоставляет пользователю возможность создания единой учётной записи для аутентификации на множестве не связанных друг с другом интернет-ресурсов, используя услуги третьих лиц?

43.Какой пароль, действителен только для одного сеанса аутентификации, действие этого пароля также может быть ограничено определённым промежутком времени?
44.Однократный ввод учетных данных для доступа к нескольким системам/приложениям, - это?
45.Какой из популярных методов взлома паролей на серверах и в различных программах, основан не переборе паролей и учетных записей?
46.Какой класс решений, обеспечивает контроль и защиту мобильных устройств, используемых организацией и её сотрудниками?
47.Набор распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей, - это?
48. Какая технология позволяет не только проверять устройства и пользователей еще на подступах к ресурсам корпоративной сети, но и предотвратить доступ компьютеров, не соответствующих политике безопасности - заражен вредоносной программой, отсутствует или устарел антивирус, отсутствуют необходимые обновления и сервис-паки, средства персональной защиты?
49.Какое средство унифицированного управления угрозами обеспечивает комплексную защиту от сетевых угроз, является модификацией обыкновенного файервола, продуктом «все включено», объединяющим в себе множество функций, связанных с обеспечением сетевой безопасности, например, системы обнаружения и предотвращения вторжений, межсетевого экрана, VPN, антивируса, средства анализа и инспектирования сетевого трафика?
50. Комплекс аппаратных и программных средств, который с заданной периодичностью копируют и резервируют определенную информацию: от конкретных файлов и папок до целых образов систем и серверов и баз данных, при инцидентах быстро восстанавливает нужные данные и позволяет продолжить работу уже через несколько минут, - это?

Блок заданий открытого типа
Формируемые ПК 3.2.

1.Как называется любая характеристика информационной системы, использование которой нарушителем может привести к реализации угрозы?
2.Событие или совокупность событий, которые применительно к каждому отдельно взятому объекту должны рассматриваться в качестве попыток совершения информационного воздействия противоправного или деструктивного характера, - это?
3.Процесс оценки подозрительных действий в защищаемой сети, который реализуется либо посредством анализа журналов регистрации операционной системы и приложений, либо сетевого трафика, - это?
4.Сколько выделяют классов систем обнаружения атак по принципу реализации и какие?
5. Какие системы обнаружения атак осуществляют мониторинг активности одного узла в сети?
6.В каких системах обнаружения атак объектом мониторинга является сетевой сегмент?
7.В каком подходе к обнаружению атак системы обнаружения атак (СОА) осуществляют поиск шаблонов известных атак в сетевом трафике или высокоуровневых данных?
8. В каком подходе к обнаружению атак системы обнаружения атак (СОА) обладают профилем нормальной активности системы и детектируют отклонения от него?
9.Какие системы обнаружения атак, состоят из множества IDS, которые расположены в различных участках большой сети, связаны между собой и с центральным управляющим сервером?
10.Какие программные или аппаратные системы сетевой и компьютерной безопасности обнаруживают вторжения или нарушения безопасности и автоматически защищают от них?
11.Решения для сбора и анализа событий, генерируемых различными типами СЗИ, - это?
12.Комплекс, предназначенный для централизованного сбора и анализа информации о событиях, поступающих из различных источников автоматизированной системы компании, - это?
13.Какая система позволяет осуществлять сравнение уязвимостей программного обеспечения с точки зрения их опасности?

14.Как называют сотрудников, которым доступна конфиденциальная информация организации,

где они работают и которые могут использовать корпоративные секреты в корыстных целях, провоцируя умышленные утечки информации?
15.Назовите два основных этапа работ по анализу защищенности, проводимых по отношению к периметру корпоративной сети?
16.Какие работы проводятся для оценки возможности преодоления механизмов защиты информации потенциальным внешним злоумышленником и получения им несанкционированного доступа к одному или нескольким информационным активам организации, расположенным на периметре и внутри корпоративной сети?
17.Какая модель потенциального злоумышленника, действующего из сети Интернет, не имеющего логических прав в ИС организации и не обладающего сведениями о корпоративной сети и ИС организации, используется в рамках работ по внешнему тестированию на проникновение?
18. Какая модель потенциального злоумышленника, имеющего типовой набор клиентских прав доступа к сервисам, предоставляемым клиенту организации, связанным с обслуживанием физических лиц, используется в рамках работ по внешнему тестированию на проникновение?
19. Какая модель потенциального злоумышленника, обладающего типовым набором прав работника, имеющего возможность использовать сервисы удаленной работы, используется в рамках работ по внешнему тестированию на проникновение?
20.Какие работы проводятся для оценки возможности преодоления механизмов защиты информации потенциальным внутренним злоумышленником и осуществления им несанкционированного доступа к одному или нескольким информационным активам организации, расположенным внутри корпоративной сети?
21.Какие программы способны перехватывать и анализировать сетевой трафик, полезны в тех случаях, когда нужно извлечь из потока данных какие-либо сведения (например, пароли), или провести диагностику сети?
22.Один из самых распространенных видов нежелательного программного обеспечения, предназначенный для несанкционированного сбора данных с пользовательского устройства, использующийся, например, для сбора информации о местоположении устройства, посещаемых сайтах, конфигурации компьютера, используемом программном обеспечении, вводимых с клавиатуры данных, - это?
23.Какие шпионские программы передают злоумышленнику данные о местоположении устройства, открываемых веб-сайтах, документах, списках контактов, маршруте передвижения, наиболее часто посещаемых местах?
24.Устройство или программное обеспечение для перехвата данных, вводимых с клавиатуры, которое распознаёт нажатия кнопок, скрыто сохраняет и передает информацию злоумышленнику - это?
25.Какие программы используются для удаленного управления рабочими станциями или другими компьютерными устройствами, с их помощью можно выполнять почти любые действия с удаленной системой: передавать файлы, вести наблюдение за действиями пользователя, производить настройки системы, управлять функциями ввода/вывода?
26.Какие системы работают внутри периметра безопасности, анализируют учётные записи, права, файлы, их содержимое, доступы и перемещения, выявляют нарушения, в автоматическом режиме выявляют и исправляют проблемы с хранением и использованием данных в компании?
27.Сотрудники компании, неискушенные в теме информационной безопасности, зачастую могут путать DoS-атаки и DDoS-атаки. Объясните, в чем отличия этих атак?
28. Процесс проверки инфраструктуры компании на наличие проблем и слабых мест, которые могут быть связаны с ошибками конфигурации, исходным кодом или используемым ПО, - это?
29. Какие программные и аппаратные средства используются для обнаружения неавторизованного входа в систему, а также неправомерных и несанкционированных попыток по управлению защищаемой сетью, применяются для дополнительного усиления уровня информационной безопасности?
30.Часть инфраструктуры, представляющую собой совокупность физических, программных, программно-аппаратных и/или логических систем и средств, выход из строя которых, либо их частичное повреждение/уничтожение могут привести к критическим последствиям для всей

инфраструктуры и/или экономического сектора, в котором эта инфраструктура реализована, - это?
31.Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа, - это?
32.Какая учетная запись имеет больше прав, чем стандартная учетная запись, однако объем прав таких записей может существенно различаться в зависимости от организации, должностных обязанностей или ролей и используемых технологий?
33.Один из этапов инцидент-менеджмента, направленный на восстановление хронологии произошедшего инцидента ИБ, выявление всех факторов, способствовавших его возникновению, в том числе причастных лиц, посредством анализа всех цифровых следов, имеющих отношение к данному инциденту и при необходимости, к данной процедуре могут быть привлечены эксперты и сотрудники правоохранительных органов, - это?
34.Процесс сбора и анализа информации об ИС и реализованных организационно-технических мерах защиты для качественной или количественной оценки уровня ее защищенности и/или установления соответствия требованиям нормативных документов, - это?
35.Совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов организации от угроз безопасности, - это?
36.Как называют комплексный показатель, характеризующий релевантность системы ИБ тем угрозам, которые могут наступить, возможность предотвратить их наступление и противостоять им и их последствиям в случае наступления, может быть выражен степенью вероятности наступления той или иной угрозы и её последствий?
37.Какая модель, описывает потенциального нарушителя безопасности и подходы по определению актуальности угроз и вероятности их наступления с учетом возможностей потенциального нарушителя и особенностей конкретной информационной системы в текущих условиях?
38.Какая целевая продолжительная высокоуровневая атака, проводится группировкой профессиональных киберпреступников, зачастую действующих в интересах какого-либо государства и использующих дорогостоящий инструментарий, в том числе собственной разработки?
39.Какой сетевой протокол прикладного уровня служит для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия?
40.Какой криптографический сетевой протокол служит для безопасного управления сетевыми службами в незащищенной сети?
41.Как называют технологию поиска, аккумулирования и анализа данных, собранных из доступных источников в интернете?
42.Метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника, называют?
43.Процесс создания программной (виртуальной) версии компьютера с выделенными ресурсами ЦП, памяти и хранилища, которые "заимствуются" у физического компьютера и (или) удаленного сервера, - это?
44.Компьютерный файл (или образ), который действует как обычный компьютер, он отделен от остальной части системы, то есть его программное обеспечение не может вмешиваться в работу основной операционной системы компьютера, - это?
45.Файлы с записями о событиях в хронологическом порядке называют?
46.Характерные признаки/особенности некой сущности, позволяющие её идентифицировать, в основном применяются к функции программирования, компьютерным вирусам, либо файлам, - это?
47.В каком программном обеспечении хранится и обрабатывается информация в структурированном виде?
48.Какой программный механизм предназначен для записи, поиска, сортировки, обработки и печати информации, содержащейся в базе данных?
49.Настройка межсетевых экранов перед СУБД, чтобы заблокировать любые попытки доступа от сомнительных источников, настройка и поддержание в актуальном состоянии парольной политики и ролевой модели доступа, - это?

50.Для проведения какого мониторинга организации пользуются средствами защиты баз данных, входящими в состав СУБД, механизм проведения которого заключается в настройке и включении триггеров, а также создании специфических процедур, которые начинают срабатывать во время запроса доступа к чувствительной информации, при этом ведется журнал запросов и подключений к системе управления базами данных в виде таблицы, где указаны данные о том, в какое время, кем и какой запрос был сделан?

Блок заданий открытого типа
Формируемые ПК 3.3.

1.Когда возникает типичная ситуация, требующая несколько уровней межсетевых экранов?

2.Какие средства защиты устанавливают между общедоступной сетью (такой, как Internet) и внутренней сетью?

3.Какую функцию выполняет межсетевой экран?

4.Для чего нужно контролировать и регулировать доступ пользователей внутренней сети к ресурсам общедоступной сети?

5.Для чего необходимо ограничивать доступ во внутреннюю сеть со стороны общедоступной сети за счет применения фильтров и средств аутентификации?
6.На какие группы можно разделить все межсетевые экраны по способу их реализации?
7.Каким образом работает с трафиком фильтр пакетов?
8.Свободная реализация технологии VPN с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиент, позволяющая устанавливать соединения между компьютерами, находящимися за NAT-firewall, без необходимости изменения их настроек, - это?
9.Какой туннельный протокол типа точка-точка, позволяет компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети?
10.К каким виртуальным сетям могут подключаться «внешние» пользователи - клиенты или заказчики, имеющие меньшее доверие, нежели сотрудники компании, и существует необходимость создания определенных правил, ограничивающих доступ «внешних» пользователей к конфиденциальной или коммерческой информации?
11.Какие виртуальные сети реализуются для обеспечения защищенного канала между корпоративной сетью и пользователем, подключенным к защищенной сети извне, например, с домашнего ПК?
12.Какие VPN реализуются провайдерами для предоставления доступа клиентам, подключающимся по одному физическому каналу?
13.Какая VPN объединяет в защищенную сеть ряд филиалов одной компании, распределенных географически, для обмена информацией по открытым каналам?
14.Какая VPN защищает данные, передаваемые между узлами корпоративной сети (но не сетями), обычно реализуется для узлов, находящихся в одном сетевом сегменте, например, клиентской машиной и сервером, также применяется для разделения одной физической сети на несколько логических?
15.Задача обеспечения доступности внешних ресурсов компании всегда была актуальна для организаций, продающих свои товары и услуги через сайты. Недоступность сайта может привести и к финансовым потерям - в виде недополученной прибыли или снижения клиентопотока, - и к имиджевым. Самым эффективным вредоносным инструментом, с помощью которого злоумышленники могут вызвать подобную недоступность, являются атаки, во время которых генерируются миллионы запросов, «подвешивающих» серверы и приложения. Как называют эти атаки?

16.Долгое время при безопасном удалённом доступе к инфраструктурам организаций вместе с российскими криптоалгоритмами применялась схема с созданием защищённых VPN-туннелей на сетевом уровне. Для этого было необходимо разворачивать VPN-клиенты на рабочих местах пользователей и организовывать сетевые соединения до шлюза. Поскольку основными целями удалённого доступа являются корпоративные веб-приложения, развёртывание VPN-туннелей для таких задач видится избыточным. По какому протоколу можно организовать защищённый доступ в данном случае?
17.Какой криптографический протокол обеспечивает защищённую передачу данных между узлами в сети Интернет?
18.Каковы основные функции протокола TLS?
19. Какие программные или программно-аппаратные средства обеспечивают охрану данных от возможной утечки внутри компании, - анализируют все исходящие и иногда входящие информационные потоки, создавая защищенный цифровой периметр, контролируют не только веб-трафик, но и распечатанные или отправляемые по wi-fi и bluetooth документы?
20. Какие программные или программно-аппаратные средства, позволяют осуществлять запуск операционной системы исключительно с доверенных носителей информации (например, жестких дисков), при этом такие устройства могут производить контроль целостности программного обеспечения (системных файлов и каталогов операционной системы) и технических параметров (сравнивать конфигурации компьютера при запуске с теми, которые были предопределены администратором при инициализации), выступать в роли средств идентификации и аутентификации (с применением паролей и токенов)?
21.Какие программные и/или аппаратные средства, позволяют предотвратить попытки несанкционированного доступа, такие как неавторизованный физический доступ, доступ к файлам, хранящимся на компьютере, уничтожение конфиденциальных данных?
22.Какие средства защиты могут выполнять функции идентификации и аутентификации пользователей и устройств; регистрацию запуска (завершения) программ и процессов; реализацию необходимых методов (дискреционный, мандатный, ролевой), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; управление информационными потоками между устройствами; учет носителей информации и другие функции?
23.Какие аппаратные, программные и аппаратно–программные средства, системы и комплексы реализуют алгоритмы криптографического преобразования информации, предназначены для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении?
24.Какие средства безопасности предназначены для анализа защищенности информации в корпоративных сетях и могут выполнять функции проверки сетевых устройств; проверки возможности осуществления атак типа "Denial of Service", "Spoofing"; проверки паролей; проверки межсетевых экранов; проверки удаленных сервисов; проверки DNS; проверки учетных записей ОС; проверки сервисов ОС; проверки установленных patch'ей системы безопасности ОС?
25.При сравнении межсетевых экранов, помимо цены и наличия сертификата ФСТЭК, необходимо обращать внимание на функциональную составляющую и выбирать не просто межсетевые экраны, а полноценные сетевые шлюзы безопасности, состоящие из шлюзового антивируса; блокировки сайтов по их содержимому, категории или конкретному адресу; VPN (возможность создания виртуальных частных сетей); мониторинга сетевой активности и отчетность; управления пропускной способностью интернет-доступа. Как называются такие решения?
26.Какое решение по защите от вирусной угрозы используют для защиты пользователей от угроз, приходящих извне (с веб-сайтов и зараженных файлов, скачиваемых через веб-браузер)?
27.Какая система безопасности защищает от негативного воздействия внешних злоумышленников на компьютерную сеть организации, а именно от использования уязвимостей в сетевых протоколах, DoS-атак, сетевого сканирования, работы ботнетов и скомпрометированных хостов, работы хостов, зараженных троянским ПО и сетевыми червями, использования скомпрометированных SSL-сертификатов, спам-сетей?

28.Какую технологию используют для объединения компьютерных сетей организации,

географически удаленных друг от друга, в основе этой технологии заложен принцип шифрования данных, передаваемых через публичную сеть интернет, другими словами, никто, кроме участников, не сможет открыть эти данные и воспользоваться ими?
29. К какому виду программно-технических способов и средств обеспечения информационной безопасности относят средства авторизации; мандатное управление доступом; избирательное управление доступом; управление доступом на основе ролей; журналирование (так же называется аудит)?
30. К какому виду программно-технических средств обеспечения информационной безопасности относят системы обнаружения и предотвращения вторжений (IDS/IPS) и системы предотвращения утечек конфиденциальной информации (DLP-системы)?
31. К какому виду программно-технических средств обеспечения информационной безопасности относят шифрование и цифровую подпись?
32. К какому виду программно-технических способов и средств обеспечения информационной безопасности относят пароль; ключ доступа (физический или электронный); сертификат; биометрию?
33. К какому виду программно-технических способов и средств обеспечения информационной безопасности относят источники бесперебойного питания; резервирование нагрузки; генераторы напряжения.
34.Хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам, называется?
35. Какие программные или программно-аппаратные средства собирают исходящий, входящий и внутрикорпоративный трафик организации, действия пользователей и другие события с помощью модулей-перехватчиков, далее перехваченную информацию обрабатывают с помощью политик фильтрации, контентного и контекстного анализа?
36. Важным средством защиты, заключающемся в фиксации всех событий, от которых зависит безопасность системы, например, попытки удачного и неудачного логического входа в систему, операции доступа к некоторым каталогам и файлам, использование принтеров, является?
37. В какой операционной системе содержатся перечисленные элементы защиты: встроенная система безопасности parsec; мандатное управление доступом; изоляция модулей; очистка оперативной и внешней памяти и гарантированное удаление файлов; маркировка документов; регистрация событий; защита информации в графической подсистеме?
38. Для обеспечения безопасности ОС очень важно, чтобы доверенные, обладающие высоким уровнем целостности процессы (например, работающие от имени «красного» администратора), стартовали из высокоцелостных исполняемых файлов. Поэтому запуская процессы, «красный» администратор ОС Astra Linux SE может быть всегда уверен, что используемые исполняемые файлы не модифицированы и не подменены. Какое СЗИ обеспечивает безопасность в данном случае?
39.Важным СЗИ, который в ОС Astra Linux SE целесообразно активировать, начиная с режима «Усиленный», запуск исполняемых файлов и загрузка исполняемых библиотек возможна только в том случае, если они подписаны электронной цифровой подписью на доверительном ключе. Следовательно, СЗИ обеспечивает защиту от загрузки произвольного исполняемого файла или библиотеки, не обладающих корректной ЭЦП, что значительно усложняет эксплуатацию уязвимостей, а в большинстве случаев делает ее невозможной (неэффективной). Какое СЗИ обеспечивает безопасность в данном случае?
40.Наличие МКЦ в ОС Astra Linux Special Edition дает возможность разрабатывать и внедрять технологии защиты, позволяющие создавать для недоверенного («опасного»), программного обеспечения своеобразные «песочницы», где эти приложения изолируются от остальных доверенных приложений. В таких «песочницах», работающих на пониженном уровне целостности, недоверенное программное обеспечение (например, браузер, который обрабатывает самые разные непроверенные данные из интернета), даже если подвергнется атаке нарушителя или заражению вирусом, не будет представлять опасности для всей остальной системы. Какое СЗИ обеспечивает безопасность в данном случае?

41. Российская ОС Astra Linux может стать полноценным аналогом для бизнеса, пользующегося Windows или macOS. Поясните, в чем главное преимущество системы Astra Linux перед зарубежными IT-продуктами?
42. Какая операционная система позволяет реализовать многоуровневую модель защиты от эксплуатации уязвимостей за счет одновременного применения мандатного контроля целостности, замкнутой программной среды и ограничения программной среды посредством механизмов системного киоска?
43. Какая СЗИ ОС Astra Linux SE обеспечивает разделение системных компонентов операционной системы по уровням доверия, существенно сокращая поверхность атаки для злоумышленника, так как за счет применения указанной технологии даже использование уязвимости в ряде системных компонентов (графический сервер, сетевые сервисы, средства виртуализации) не приведет к полной компрометации системы и скрытии следов взлома?
44. Какие инструменты защиты ОС Astra Linux SE предоставляют возможность внедрения цифровой подписи в исполняемые файлы формата ELF, входящие в состав устанавливаемого ПО и в расширенные атрибуты файловой системы, что позволяет реализовать запрет на открытие файлов и загрузки модулей ядра, поставленных на контроль, с неверной электронной подписью или без неё?
45. Соответствует ли операционная система Astra Linux Special Edition требованиям регуляторов, если да, то каких?
46. Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, -это?
47. В состав какой российской ОС входит специализированная подсистема распределенного аудита, позволяющая отслеживать критичные события безопасности в корпоративной сети и предоставляющая нужные инструменты для оперативного реагирования на инциденты информационной безопасности?
48. В состав какой серверной российской ОС входит модульная платформа конфигурирования с графическим и веб-интерфейсом (Alterator)?
49.Возможности привилегированных учетных записей часто используют при взломах и кражах ценной конфиденциальной информации. Привилегированными пользователями могут быть топ-менеджеры, администраторы, напрямую работающие с информационными системами, и подрядчики, имеющие расширенный доступ в корпоративную сеть. Отсутствие автоматизированных инструментов приводит к тому, что сотрудники ИБ тратят много времени на контроль подобных аккаунтов. Какая система безопасности позволяет оптимизировать обработку и мониторинг действий учетных записей с повышенными привилегиями?
50.В условиях цифровизации практически всех бизнес-процессов, любое взаимодействие с информацией становится не только проще, но и более рискованным. С каждым днем появляется все больше способов получить несанкционированный доступ к конфиденциальным данным, и поэтому их сохранность является одним из важнейших приоритетов для любой компании. Какие средства защиты используют для обеспечения подобной безопасности?