СОГЛАСОВАНО
Начальник отдела защиты информации
Департамента цифрового развития
Смоленской области
_____ А.Н. Калугин
«31» 08 2022 г.

УТВЕРЖДАЮ
Заместитель директора по
учебной работе
_____ И. В. Иванешко
«31» 08 2022 г.

Контрольно-оценочные средства для промежуточной аттестации УП 03.01 Учебная практика, ПП 03.01 Производственная практика по профессиональному модулю ПМ.03 Обеспечение информационной безопасности систем мобильной связи по специальности11.02.08 – Средства связи с подвижными объектами

Комплексный дифференцированный зачет является промежуточной формой контроля, подводит итог освоения УП.03.01, ПП.03.01, проверяет сформированность следующих профессиональных компетенций:

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

А также общих компетенций:

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 команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), 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

Промежуточный контроль по учебной и производственной практикам осуществляется в виде комплексного дифференцированного зачета (учебная и производственная практика в совокупности).

Комплексный дифференцированный зачет по УП.03.01 и ПП.03.01 проводится на основе тестирования по учебной практике, а также предоставленных документов: отчета по производственной практике в соответствии с требованиями оформления, дневника по практике, положительной характеристики работодателя и заполненного аттестационного листа.

Шкала перевода баллов в оценки:

Оценка результатов КДЗ	Количество баллов		
	УП.03	ПП.03 (аттестационный лист, дневник, положительное заключение работодателя)	ПП03 (отчет по практике)
«5» (отлично)	5 4	12 12	1 1
«4» (хорошо)	4 3	12 12	1 1
«3» (удовлетворительно)	3	12	1
«2» (неудовлетворительно)	2 5 4 3	Менее 12 Менее 12 Менее 12 Менее 12	0 0 0 0

В результате освоения УП.03.01 и ПП.03.01 студент должен:

Иметь практический опыт:

ПО 1 – выявления каналов утечки информации;

ПО 2 – определения необходимых средств защиты;

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

ПО 4 - разработки политики безопасности для объекта защиты;

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;

ПО 13 – использования систем и решений для борьбы с мошенничеством в сети;

ПО 14 – использования системы обнаружения вторжений с применением систем мониторинга;

ПО 15 – использования систем защиты от распределённых атак на АИС;

ПО 16 - установки, настройки специализированного программного обеспечения по защите информации в сетях мобильной связи.

Уметь:

У1 – классифицировать угрозы информационной безопасности;

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

У3 - определять возможные виды атак;

У4 - осуществлять мероприятия по проведению аттестационных работ;

У5 - разрабатывать политику безопасности объекта;

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;

У13 – использовать общую схему подключения системы фродконтроля;

У14 – использовать решения на основе технологии NAC;

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

У16 – использовать стандарты и рекомендации в области защиты виртуальных сред.

Знать:

З1 – каналы утечки информации;

З2 – назначение, классификацию и принципы работы специализированного оборудования;

З3 - принципы построения информационно-коммуникационных сетей;

З4 - возможные способы несанкционированного доступа;

З5 - законодательные и нормативные правовые акты в области информационной безопасности;

З6 - правила проведения возможных проверок;

З7 - этапы определения конфиденциальности документов объекта защиты;

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.

З14 – виды мошенничества в телекоммуникациях;

З15 – принципы детектирования предфродового состояния;

З16 – принципы обеспечения информационной безопасности в VoIP сетях;

З17 - угрозы информационной безопасности, актуальные для виртуальных сред.

Тест содержит 20вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока (первый блок 150 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.

Образцы аттестационных листов по практикам (приложение 1, приложение 4), требования к оформлению технического отчета (приложение 2), дневника практики, характеристики работодателя (приложение 3), ведомости (приложение 5) приводятся в приложениях.

Результаты определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», вносятся в итоговую ведомость комплексного дифференцированного зачета и объявляются в тот же день.

Шкала оценивания образовательных результатов тестирования:

Критерии	Кол-во баллов по тестированию
получают студенты, справившиеся с работой 100-90%;	5 баллов
получают студенты, справившиеся с работой 89-76%	4 балла
получают студенты, справившиеся с работой 60-75%	3 балла
менее 60% правильных ответов	От 0 до 2 баллов

Блок заданий закрытого типа Формируемые ПК 3.1, ОК 1 – ОК 9		
1.	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.
2.	Каковы основные угрозы доступности информации?	1.Непреднамеренные ошибки пользователей. 2.Злонамеренное изменение данных 3.Хакерская атака. 4.Отказ программного и аппаратного обеспечения. 5.Разрушение или повреждение помещений. 6.Перехват данных.
3.	Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?	1.Доступность 2.Целостность 3.Конфиденциальность 4.Управляемость 5.Надежность
4.	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.
5.	Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется?	1.Мониторинг. 2.Аудит. 3.Управление ресурсами. 4.Администрирование.
6.	Что относится к угрозам информационной безопасности?	1.Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию. 2.Классификация информации. 3.Стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.). 4.Сбои и отказы оборудования (технических средств) АС. 5.Ошибки эксплуатации. (пользователей, операторов и другого персонала). 6.Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов). 7.Последствия ошибок проектирования и разработки компонентов АС. (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.). 8.Иерархическое расположение данных.
7.	Каким образом функционируют системы обнаружения атак на уровне узла?	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.
8.	Каким образом функционируют системы обнаружения атак на уровне сети?	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.
9.	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.
10.	Как классифицируется информация по доступности?	1.Открытую информацию и государственную тайну. 2.Конфиденциальную информацию и информацию свободного доступа. 3.Информацию с ограниченным доступом и общедоступную информацию. 4.Виды информации, указанные в остальных пунктах.
11.	Задачей анализа модели политики безопасности на основе анализа угроз системе является?	1.Минимизация вероятности преодоления системы защиты. 2.Максимизация затрат для взлома. 3.Максимизация ресурса для взлома. 4.Максимизация времени взлома.
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.	Какую возможность вычислительной системе дает идентификация пользователя?	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.	В чем состоит основное назначение межсетевого экрана? (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 внешнее окружение на функционирование межсетевого экрана, относятся?	1.Используемые транспортные протоколы (IPv4 или IPv6). 2.Количество отделов в организации. 3.Специфика защищаемых сервисов. 4.Количество комнат в помещении.
25.	Политиками по умолчанию для	1.Запретить весь входящий трафик, который явно не

	межсетевого экрана считаются?	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.	Какие из утверждений являются верными?	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.	Какие из утверждений являются верными?	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.	Что такое анализ защищенности ИТ-инфраструктуры?	1.Анализ защищенности – это неконтролируемое техническое воздействие, направленное на выявление минимального количества уязвимостей в исследуемой

		ИТ-инфраструктуре. 2.Анализ защищенности – это контролируемое техническое воздействие, направленное на выявление максимального количества уязвимостей и недостатков в исследуемой ИТ-инфраструктуре или информационной системе. 3.Анализ защищенности – это организационное воздействие, направленное на выявление потерь от угрозы информационной безопасности в исследуемой ИТ-инфраструктуре или информационной системе.
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.	Что является основными компонентами управления доступом?	1.Субъекты. 2.Маршрутизаторы. 3.Объекты или ресурсы. 4.Разрешения (привилегии).
47.	Какие компоненты входят в состав политики безопасности?	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.	Что определяет собственник информационных активов при разработке политики безопасности в первую очередь?	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.	Какой руководящий документ используют для определения требуемого класса защищенности?	1.«Классификация автоматизированных систем и требований по защите информации» Часть 1. 2.«Классификация автоматизированных систем и требований по защите информации» Часть 2. 3.Федеральный закон от 26 июля 2017 г. №187-ФЗ О безопасности критической информационной инфраструктуры Российской Федерации».
50.	Какие правила использования ресурсов сети применяют для разграничения доступа на уровне файловой системы?	1.Правила фильтрации 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, ОК 1 – ОК 9		
1.	Какие задачи решаются при проведении анализа защищенности?	1.Выполнение требований регуляторов. 2.Получение представления о текущем уровне защищенности системы. 3.Оценка защищенности ИТ-инфраструктуры и эффективности используемых механизмов защиты. 4.Получение подробной картины уязвимостей и недостатков исследуемой системы.

		5.**Все,** перечисленное в остальных пунктах.
2.	Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы – это?	1.Аутентификация. 2.Идентификация 3.Аудит 4.Авторизация
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.	Когда рекомендуется проводить работы по анализу защищенности?	1.При первичной установке информационной системы. 2.При публикации новой версии используемой ИС. 3.При внесении существенных изменений в систему или инфраструктуру. 4.По прошествии длительного периода времени с последней проверки. 5.Все, перечисленное в остальных пунктах.
9.	Сколько классов защищенности автоматизированных систем от несанкционированного доступа к информации выделено в Руководящем документе ГТК «Классификация автоматизированных систем и требований по защите информации», часть 1?	1. 6 классов защищенности. 2. 7 классов защищенности. 3. 9 классов защищенности. 4. 5 классов защищенности. 5. 8 классов защищенности.
10.	Сколько классов защищенности средств вычислительной техники	1. 6 классов защищенности. 2. 7 классов защищенности.

	установлено в Руководящем документе ГТК?	3. 9 классов защищенности. 4. 5 классов защищенности. 5. 8 классов защищенности.
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.	Какой документустанавливает требования, спецификации, руководящие принципы, в соответствии с которыми могут использоваться материалы, продукты, процессы и услуги, которые подходят для этих целей?	1. Нормативно-методический документ. 2.Стандарт. 3.Руководящий документ. 4. Нормативно правовой акт.
13.	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию, называется?	1. Нормативно-методические документы. 2.Электронная подпись 3. Критическая информационная инфраструктура. 4.Хэш-фунция.
14.	Какой из предложенных вариантов пароля "правильный" (с точки зрения современных требований к паролю)?	1.1rR%56ty. 2.i23Y65. 3.mersqwertyp. 4.3488714567747865.
15.	Как называется некоторая уникальная информация, позволяющая различать пользователей?	1.Идентификатор (логин). 2.Пароль. 3.Учетная запись. 4.Ключ.
16.	Как называетсясекретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе?	1.Идентификатор (логин). 2.Пароль. 3.Учетная запись. 4.Ключ.
17.	Как называетсясовокупность идентификатора и пароля пользователя?	1.Логин пользователя. 2.Учетная запись пользователя. 3.Ключ пользователя.
18.	Как называетсяприсвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку?	1.Идентификацией пользователя. 2.Аутентификацией пользователя. 3.Опознанием пользователя. 4.Созданием учетной записи пользователя.
19.	Как называетсяпроверка принадлежности пользователю предъявленного им идентификатора?	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.	Какая электронная подпись (ЭП) однозначно подтверждает, что данное электронное сообщение отправлено конкретным лицом?	1.Усиленая неквалифицированная ЭП. 2. Усиленная квалифицированная ЭП. 3. Простая ЭП. 4.Сложная ЭП.

22.	Какой атакой на ИС является невозможность получения сервиса законным пользователем?	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.	Что могут определять атаки сканирования?	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.	Какая электронная подпись (ЭП) позволяет не только однозначно идентифицировать отправителя, но и подтвердить, что с момента подписания документа его никто не изменял?	1.Усиленая неквалифицированная ЭП. 2. Усиленная квалифицированная ЭП. 3. Простая ЭП. 4.Сложная ЭП.
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.	Что должно располагаться в сети демилитаризованной зоны (DMZ)?	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, 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.	Каково 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.	Каково оптимальное количество DMZ, если в организации есть веб-сервер для внешних пользователей и веб-сервер для получения информации своими сотрудниками?	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.«Отказотобслуживания» (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.«Отказотобслуживания» (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.«Отказотобслуживания» (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.«Отказотобслуживания» (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.	Какие параметры 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.	Что происходит в ИС при использовании IDS?	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.	Каким образом могут быть реализованы IDS?	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 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.
49.	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.
50.	На основании чего осуществляется управление доступом в пакетном фильтре?	1.IP-адрес источника. 2.IP-адрес назначения. 3.Номер привила в наборе правил пакетного фильтра. 4.Учетная запись и пароль пользователя.
Блок заданий закрытого типа Формируемые ПК 3.3, ОК 1 – ОК 9		
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.	Что является объектом доступа в системах управления доступом?	1.Файл. 2.Любой сетевой ресурс, к которому субъект хочет получить доступ. 3.Аппаратное устройство. 4.Прикладная система. 5.Все ответы верны.
4.	Что следует использовать для разграничения трафика при управлении доступом на сетевом уровне?	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.	Что из перечисленного не позволяет реализовать технология VLAN?	1.Выполнять шифрование трафика. 2.Выполнять фильтрование пакетов, основываясь на правилах. 3.Выполнять аутентификацию на уровне пользователя. 4.Предотвратить широковещательные штормы.
7.	Что из перечисленного позволяет реализовать технология VLAN?	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.	Что позволяет реализовать трансляция сетевых адресов (NAT)?	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.
9.	Где используется NAT?	1.В IPv4. 2.В IPv6. 3.В IPv32. 4.В IPv64.
10.	Что позволяет реализовать использование технологии VLAN?	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.	За счет чего повышается безопасность ИС при использовании технологии VLAN?	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.	Какие функции могут выполнять межсетевые экраны прикладного уровня?	1.Выполнять аутентификацию пользователя. 2.Автоматически распознавать новые протоколы. 3.Шифровать данные пользователя. 4.Выполнять авторизацию пользователя.
13.	Какие функции не могут выполнять межсетевые экраны прикладного уровня?	1.Выполнять аутентификацию пользователя. 2.Автоматически распознавать новые протоколы. 3.Шифровать данные пользователя. 4.Выполнять авторизацию пользователя.
14.	Что понимают под унифицированным управлением угрозами (Unified Threat Management – UTM)?	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.
15.	Какой трафик обрабатывают выделенные прокси-серверы?	1.Конкретного уровня модели OSI. 2.Конкретного прикладного протокола. 3.Конкретного адреса отправителя. 4.Конкретного пользователя.
16.	В чем заключается 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.	В чем основное отличие прокси-шлюзов прикладного уровня?	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.	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.
19.	Что определяет процедура управления пользователями?	1.Кто может осуществлять авторизованный доступ к тем 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.	Каким образом может осуществляться администрирование межсетевого экрана?	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.
24.	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.
25.	Каковы основные функции у межсетевых экранов, расположенных на границе сетевого периметра?	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.
26.	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?	1.Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования. 2.Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации. 3.Улучшить контроль за безопасностью этой информации. 4.Снизить уровень классификации этой информации.
27.	Для каких целей 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.
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.	Какие объекты относятся к критической информационной инфраструктуре (КИИ)?	1. Информационные системы. 2. Телекоммуникационные сети. 3.Автоматизированные системы управления технологическими процессами. 4. Все, перечисленное в остальных пунктах.
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 основные цели технической защиты информации?	1. Защита информации с помощью ее криптографического преобразования. 2.Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств. 3.Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
33.	Для каких систем пригодна статическая NAT?	1.Для любых систем. 2.Для систем в DMZ. 3.Для клиентских рабочих станций.
34.	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.
35.	Для каких целей устанавливается IDS?	1.Обнаружение атак 2.Предотвращение атак

		3.Обнаружение нарушений политики 4.Повышение надежности системы.
36.	Какого типамежсетевые экраны устанавливают на физическом периметре информационных систем?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
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.	Какого типамежсетевые экраны устанавливаются на логической границе информационных систем?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
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	1.Определить типы трафика, которые необходимы

	разработкой политики межсетевого экранирования?	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.	Какого типамежсетевые экраны осуществляют разбор http(s)-трафика между веб-сервером и клиентом?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
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 специальными электронными схемами по определенным логическим правилам?	1.Аппаратный. 2.Программный. 3.Ручной. 4.Электромеханический.
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, ОК 1 – ОК 9

1. Как называется процедура распознавания субъекта в процессе регистрации в системе?

2.Как называетсяпроцедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует?

3.Как называетсяпроцедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации?

4.С какой целью проводится анализ защищенности?

5.Какие средства чаще всего используются для проведения анализа защищенности?

6.Какие СЗИ выявляют и соответствующим образом реагируют на средства несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации СЗИ?

7.Какие СЗИ обеспечивают меры по защите машинных носителей информации в части обеспечения контроля за их использованием?

8. Сколько классов защищенности межсетевых экранов по уровням контроля межсетевых информационных потоков определено ФСТЭК?

9. Сколько уровней защиты содержит классификация межсетевых экранов по классам защиты?

10.Какие типы межсетевых экранов определены ФСТЭК России?

11. Где устанавливаются межсетевые экраны типа «А»?

12. Где устанавливаются межсетевые экраны типа «Б»?

13. Где устанавливаются межсетевые экраны типа «В»?

14. Какого типа межсетевые экраны осуществляют разбор http(s)-трафика между веб-сервером и клиентом, и где они устанавливаются?

15.Сколько уровней защиты содержит классификация средств защиты систем обнаружения вторжений?

16.Где подключается система обнаружения вторжений уровня сети и что она контролирует?

17.Где устанавливается система обнаружения вторжений уровня узла и что она анализирует?

18.Сколько уровней защиты содержит классификация защищенности средств антивирусной защиты информации?

19. Какие типы средств антивирусной защиты Вы знаете?

20.Сколько установлено классов защиты средств доверенной загрузки?

21. Какие типы средств доверенной загрузки выделено ФСТЭК?

22.Метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает более эффективную защиту аккаунта, называется?

23.При каком методе идентификации пользователя первый рубеж - это логин и пароль, второй - специальный код, приходящий по SMS или электронной почте?

24.При каком способе аутентификации используются аутентификационные факторы нескольких типов.

25. Сколько установлено классов защиты средств контроля съемных машинных носителей?

26.Какие выделяются типы средств контроля съемных машинных носителей информации?

27. Сколько установлено классов операционных систем для обеспечения защиты информации?

28. Какие различают типы операционных систем, используемых в целях обеспечения защиты информации?

29. Где устанавливаются операционные системы типа «А»?

30. Где устанавливаются операционные системы типа «Б»?

31. Для каких целей предназначены операционные системы типа «В»?

32.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?

33.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?

34.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?

35.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?

36.Как называетсясовокупность технических средств, направленных на контроль входа и выхода в помещение с целью обеспечения безопасности и регулирования посещения определённого объекта?

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

38.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?

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

40.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?

41. 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?

42.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?

43.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?

понент управления доступомтребует от пользователей подтверждения своей личности с использованием как минимум двух или более различных факторов проверки, прежде чем получить доступ к какому-либо ресурсу?

45.Какой открытый стандартдецентрализованнойсистемыаутентификациипредоставляет пользователю возможность создания единой учётной записи для аутентификации на множестве не связанных друг с другоминтернет-ресурсов, используя услуги третьих лиц?

46.Какой пароль, действителен только для одного сеанса аутентификации, действие этого пароля также может быть ограничено определённым промежутком времени?

47.Как называетсятехнология однократного ввода учетных данных для доступа к нескольким системам/приложениям?

48.Какой из популярных методов взлома паролей на серверах и в различных программах, основан не переборе паролей и учетных записей?

49.Какой класс решений, обеспечивает контроль и защиту мобильных устройств, используемых организацией и её сотрудниками?

50.Как называетсянабор распределённых служб и компонентов, используемых для поддержки криптозадач, на основе закрытого и открытого ключей?

Блок заданий открытого типа
Формируемые ПК 3.2, ОК 1 – ОК 9

1. 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?

2.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?

3. Как называют комплекс аппаратных и программных средств с заданной периодичностью копирует и резервирует определенную информацию: от конкретных файлов и папок до целых образов систем, серверов и баз данных, при инцидентах быстро восстанавливает нужные данные и позволяет продолжить работу уже через несколько минут?

4.Как называется любая характеристика информационной системы, использование которой нарушителем может привести к реализации угрозы?

5.Как называют событие или совокупность событий, которые применительно к каждому отдельно взятому объекту должны рассматриваться в качестве попыток совершения информационного воздействия противоправного или деструктивного характера?

6.Как называется процесс оценки подозрительных действий в защищаемой сети, который реализуется либо посредством анализа журналов регистрации операционной системы и приложений, либо сетевого трафика?

7.Сколько выделяют классов систем обнаружения атак по принципу реализации и какие?

8. Какие системы обнаружения атак осуществляют мониторинг активности одного узла в сети?

9.В каких системах обнаружения атак объектом мониторинга является сетевой сегмент?

10.В каком подходе к обнаружению атак системы обнаружения атак (СОА) осуществляют поиск шаблонов известных атак в сетевом трафике или высокоуровневых данных?

11. В каком подходе к обнаружению атак системы обнаружения атак (СОА)обладают профилем нормальной активности системы и детектируют отклонения от него?

12.Какие системы обнаружения атак, состоят из множества IDS, которые расположены в различных участках большой сети, связаны между собой и с центральным управляющим сервером?

13.Какие программные или аппаратные системы сетевой и компьютерной безопасности обнаруживают вторжения или нарушения безопасности и автоматически защищают от них?

14. Что подтверждает простая ЭП?

15.Что подтверждает усиленная неквалифицированная ЭП?

16.Что подтверждает усиленная квалифицированная ЭП?

17.Как называют два основных этапа работ по анализу защищенности, проводимых по отношению к периметру корпоративной сети?

18.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?

19.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?

20. 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?

21. Какая модель потенциального злоумышленника,обладающего типовым набором прав работника, имеющего возможность использовать сервисы удаленной работы, используется в рамках работ по внешнему тестированию на проникновение?

22.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?

23.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?

24.Как называют 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, вводимых с клавиатуры данных?

25.Какие шпионские программы передают злоумышленнику данные о местоположении устройства, открываемых веб-сайтах, документах, списках контактов, маршруте передвижения, наиболее часто посещаемых местах?

26.Как называется устройство или программное обеспечение для перехвата данных, вводимых с клавиатуры, которое распознаёт нажатия кнопок, скрыто сохраняет и передает информацию злоумышленнику?

27.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?

28.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?

29.Сотрудники компании, неискушенные в теме информационной безопасности, зачастую могут путать DoS-атаки и DDoS-атаки. Объясните, в чем отличия этих атак?

30. Как называется процесс проверки инфраструктуры компании на наличие проблем и слабых мест, которые могут быть связаны с ошибками конфигурации, исходным кодом или используемым ПО?

31.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?

32.Как называют часть инфраструктуры, представляющую собой совокупность физических, программных, программно-аппаратных и/или логических систем и средств, выход из строя которых, может привести к критическим последствиям для всей инфраструктуры и/или экономического сектора, в котором эта инфраструктура реализована?

33. Как называется единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа?

34.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?

35.Как называется этап 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?

36.Как называется 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?

37.Как называют совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов организации от угроз безопасности?

38.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?

39.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?

40.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?

41.Какой сетевой протокол прикладного уровня служит для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия?

42.Какой криптографический сетевой протокол служит для безопасного управления сетевыми службами в незащищенной сети?

43.Какой метод оценки безопасности компьютерных систем или сетей использует средства моделирования атаки злоумышленника, называют?

44.Как называется процесс создания программной (виртуальной) версии компьютера с выделенными ресурсами ЦП, памяти и хранилища, которые "заимствуются" у физического компьютера и (или) удаленного сервера?

45.Как называется компьютерный файл (или образ), который действует как обычный компьютер, отделен от остальной части системы, то есть его программное обеспечение не может вмешиваться в работу основной операционной системы компьютера?

46.Как называют файлы с записями о событиях в хронологическом порядке?

47.Как называют характерные признаки/особенности некой сущности, позволяющие её идентифицировать, в основном применяются к функции программирования, компьютерным вирусам, либо файлам?

48. В каком программном обеспечении хранится и обрабатывается информация в структурированном виде?

49.Какой программный механизм предназначен для записи, поиска, сортировки, обработки и печати информации, содержащейся в базе данных?

50.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?

Блок заданий открытого типа
Формируемые ПК 3.3, ОК 1 – ОК 9

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.Как называется 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?

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 злоумышленникимогут 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

попыткинесанкционированногодоступа, такие как неавторизованный физическийдоступ,доступк 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 функциипроверки 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 изшлюзового 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 (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.Как называют хранимую в компьютерной системе совокупность данных о пользователе, необходимую для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам?

35.Какие программные или программно-аппаратные средствасобирают 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.Как называют технологию поиска, аккумулирования и анализа данных, собранных из доступных источников в интернете?

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; защитаинформации 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. 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. Какое СЗИ в ОС Astra Linux SE 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)?

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 ПО, 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 Linuxможет 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. Какое СЗИ ОС Astra Linux SEобеспечивает разделение системных компонентов операционной системы по уровням доверия, существенно сокращая поверхность атаки для злоумышленника?

44. Какие инструменты защиты ОСAstra Linux SE предоставляют возможность внедрения цифровой подписи в исполняемые файлы формата ELF, входящие в состав устанавливаемого ПО и в расширенные атрибуты файловой системы?

45. Соответствует ли операционная система Astra Linux Special Edition требованиям регуляторов, - если да, то каких?

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

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. 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?

Составил преподаватель Грубник Е.М.

Заведующий практикой Драницина М.Д.

РАССМОТРЕНО
на заседании методической
комиссии дисциплин
средств подвижной связи
Председатель _____Е.Н. Кожекина
Протокол №__ _____20__ г.

Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

СМОЛЕНСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ (ФИЛИАЛ) СПбГУТ
(СКТ(ф)СПбГУТ)

АТТЕСТАЦИОННЫЙ ЛИСТ ПО УЧЕБНОЙ ПРАКТИКЕ

_____
ФИО

Обучающийся(аяся) на 3 курсе в группе _____ по специальности СПО

11.02.08 Средства связи с подвижными объектами
код *наименование*

успешно прошел(ла) **учебную** практику по профессиональному модулю

ПМ.03 Обеспечение информационной безопасности систем мобильной связи
наименование профессионального модуля

в объеме 36 часов с ___ _____ 202__ по ___ _____ 202__ в организации

Смоленский колледж телекоммуникаций (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»
наименование организации

г. Смоленск, ул. Коммунистическая, д.21
юридический адрес

Виды и качество выполнения работ

Виды работ, выполненных студентом во время практики	***Отметка о выполнении***
1. Реализация политик безопасности в системах и сетях на примере дискреционных и мандатных прав доступа (6 часов). 2. Проведение анализа защищенности объекта защиты информации(6 часов). 3. Проведение инструментальных проверок объекта защиты информации (6 часов). 4. Сканирование портов, идентификация ОС, использование DNS для обнаружения и выяснения назначения сетевых узлов при проведении инструментальной проверки(6 часов). 5. Обеспечение безопасности сетевых операционных систем (6 часов). 6. Управления системой обнаружения вторжений на примере программного комплекса "Континент" (6 часов).	
Количество баллов по тестированию: _____	

Характеристика учебной и профессиональной деятельности студента во время учебной практики.
Аттестуемый(ая) продемонстрировал(а) / не продемонстрировал(а) владение общими и профессиональными компетенциями:

Код	Наименование результата обучения
ПК 3.1.	Использовать программно-аппаратные средства защиты информации в системах мобильной связи.
ПК 3.2.	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.
ПК 3.3.	Обеспечивать безопасное администрирование систем и сетей.
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 команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), 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.

Дата _____.
Подпись(и) руководителя(ей) практики

Преподаватель _____
подпись *расшифровка подписи*
Преподаватель _____
подпись *расшифровка подписи*

Заведующий практикой М.Д. Драницина

Приложение 2

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

СМОЛЕНСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ (ФИЛИАЛ) СПбГУТ
(СКТ(ф)СПбГУТ)

ТЕХНИЧЕСКИЙ ОТЧЕТ
по производственной практике

студента _____
ФИО

ПМ. 03 Обеспечение информационной безопасности систем мобильной связи

по специальности 11.02.08 Средства связи с подвижными объектами

г.Смоленск
20___ г.

Т Р Е Б О В А Н И Я
ПО СОСТАВЛЕНИЮ ТЕХНИЧЕСКОГО ОТЧЕТА
ПО ПРАКТИКЕ

1. Технический отчет по производственной практике студенты пишут во время прохождения практики в соответствии с графиком учебного процесса.
2. Технический отчет должен быть выполнен на стандартных листах писчей бумаги (ф. А 4), в объеме 10-12 страниц.
3. Перечень вопросов технического отчета следующий:

- титульный лист
- программа практики
- введение
- 1.Общие сведения о функциях и структуре предприятия (схема структуры предприятия)
- 2.Описание производственного процесса участка, на котором проходит основной период производственной практики.
- 3.Индивидуальное задание по ПМ.
- 4.Организация и состояние охраны труда на предприятии.
- Список литературы.
- Приложение (фото, аудио-файлы при их наличии).

4. Технический отчет должен быть оформлен в соответствии с требованиями (СТО 1.1-2015) – требования к выполнению текстовых документов:

- Текст отчета должен быть выполнен на компьютере с одинаковым межстрочным интервалом (1,0).
- Отчет выполняется на листах с одной стороны, разборчиво, аккуратно, четко.
- Текст набирается нежирным шрифтом Times New Roman на стандартных листах 14 шрифтом с соответствующей рамкой, границы которой располагаются следующим образом:

- расстояние слева от границы листа до рамки – 20мм.
- расстояние сверху, справа и снизу от границы листа до рамки 5 мм.

- Текст каждого листа записи должен иметь следующие поля:

- расстояние слева от текста до рамки 5мм, справа от текста до рамки 3мм.
- расстояние от заголовка, верхней и нижней строки текста до рамки 10 мм.
- абзацы в тексте начинаются отступом 15мм.

- В отчет обязательно должны входить структурные, функциональные схемы.
- Нумерация страниц обязательна.

5. Технический отчет должен быть проверен и подписан руководителем практики от предприятия и заверен печатью.
6. Технический отчет сдается заведующему практикой от колледжа для получения комплексного дифференциального зачета.

Заведующий практикой Драницина М.Д.

Утверждаю
Зам.директора по учебной работе

_____ Иванешко И.В.

ПРОГРАММА ПРАКТИКИ

Название МДК	**Виды работ в соответствии с рабочими программами МДК**	**Количество часов**
МДК 03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи МДК 03.02 Технология применения комплексной системы защиты информации	Изучение состава служб и участков предприятия, правила внутреннего распорядка, организация мероприятий по охране труда, мероприятия по охране труда при выполнении монтажных работ на высоте, требования к санитарно-защитным зонам и зонам ограничения застройки при монтаже ПРТО. Инструктаж по ТБ и охране труда. Изучение основ организации производства, труда и управления на объекте информатизации, составление карты информационной системы организации.	3
	Ознакомление с информационной системой безопасности предприятия, используемыми техническими средствами и программными продуктами, составление краткой характеристики информационной системы организации.	3
	Изучение применяемых технологий и технических средств, используемых в целях обеспечения защиты информации на объекте.	6
	Выявление каналов утечки информации на объекте защиты, составление модели каналов утечки информации.	3
	Изучение требований, предъявляемых к обеспечению информационной безопасности на объекте информатизации, разработка политик безопасности в системах и сетях.	3
	Всего	**18**

Индивидуальное задание (1-2 вопроса практического характера, составляются преподавателями данного ПМ):

1.

2

Примерные вопросы на производственную практику

1.Управление пользователями в JaCarta Management System.
2. Проверка работоспособности защитных модулей WEB ANTIFRAUD.
3. Функциональные возможности Group-IB Fraud Hunting Platform.
4. Архитектура системы аутентификации на базе JaCarta U2F.
5. Сценарии использования SafeNet Authentication Service.
6. Управление SafeNet eToken.
7. Сценарии использования Silverfort.
8. Функциональные возможности и работа с ESET Secure Authentication 3.0.
9. Функциональные возможности и блокировка сайтов SkyDNS.
10. Сценарии использования FortiIsolator.
11. Функциональные возможности и развертывание «Гарда БД 4».
12. Развертывание и настройка СЗИ ВИ Dallas Lock.
13. Управление учетными записями в СЗИ ВИ Dallas Lock.
14.Архитектура и функциональные возможности KES Cloud и KES Cloud Plus.
15. Архитектура и функциональные особенности Kaspersky Security для виртуальных сред.

16. Функциональные возможности и работа с vGate 4.1.
17. Сценарии использования СПО «Аккорд-KVM».
18. Функциональные возможности и сценарии использования McAfee Web Gateway.
19. Сценарии использования UserGate Log Analyzer.
20. Функциональные возможности и работа с Solar webProxy.
21. Применение Solar webProxy.
22. Функциональные возможности и сценарии SurfSecure.
23. Функциональные возможности и варианты подключения StormWall.
24. Функциональные возможности и сценарии работы услуги «Облачная защита от DDoS-атак» компании «МегаФон».
25. Функциональные возможности и сценарии использования AVSOFT ATHENA.
26. Технологии, используемые в KasperskyThreatManagementandDefense.
27.Архитектура и сценарии использования СЗИ НСД Dallas Lock Linux.
28. Функциональные возможности и использование программного модуля доверенной загрузки уровня UEFI BIOS ViPNet SafeBoot.
29. Функциональные возможности и практические примеры настройки «Континент» 3.9.
30. Функциональные возможности и сценарии использования СКЗИ «Квазар» для криптографической защиты каналов связи.
31. Функциональные возможности и работа с КриптоПро DSS.
32.Функциональные возможности и сценарии использования UserGate X10.
33. Функциональные возможности и работа с ИТ-активами в MaxPatrol VM.
34. Основные функциональные возможности и применение UserGate Management Center
35. Функциональные возможности и сценарии использования комплекса для защиты удалённых рабочих мест сотрудников САКУРА.
36. Функциональные возможности и сценарии использования InfoWatch Vision.
37. Основные возможности Dozor FC и работа с Dozor File Crawler.
38. Принцип работы и основные возможности IGA-системы Solar inRights.
39. Функциональные возможности и сценарии использования Ideco UTM 10.
40. Функциональные возможности универсального шлюза безопасности ИКС 7.2.

Председатель методической комиссииКожекина Е.Н.

Приложение 3

ДНЕВНИК
производственной практики

_____

ФИО

Группа

Специальность 11.02.08 Средства связи с подвижными объектами

успешно прошел(ла) **производственную практику** по профессиональному модулю:

ПМ.03 Обеспечение информационной безопасности систем мобильной связи

в объеме 18 часов с «___» _____20___г. по «___» _____20___г.

В организации

_____

адрес организации

Дата	Краткое описание работ, выполненных студентом во время практики	Отметка руководителя практики от предприятия о выполненной работе (подпись)

Последний день практики	сдача КДЗ в колледже	

Отношение студента-практиканта к работе (организация собственной деятельности), оформляется руководителем практики от предприятия

Дата _____ _____ 202__ г.

Подпись руководителя практики от предприятия _____ _____
ФИО *подпись*

Приложение 4

АТТЕСТАЦИОННЫЙ ЛИСТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

_____

ФИО

Обучающийся (аяся) на 3 курсе в группе ____ по специальности СПО

Специальность 11.02.08 **Средства связи с подвижными объектами**

успешно прошел(ла) **производственную** практику по профессиональному модулю

ПМ.03 Обеспечение информационной безопасности систем мобильной связи

в объеме 18 часов с «___» _____20___г. по «___» _____20___г.

в организации

_____

юридический адрес

Виды работ, выполненных студентом во время практики:

Изучил состав служб и участков предприятия, правила внутреннего распорядка, организацию мероприятий по охране труда, мероприятия по охране труда при выполнении монтажных работ на высоте, требования к санитарно-защитным зонам и зонам ограничения застройки при монтаже ПРТО. Прошел инструктаж по ТБ и охране труда. Изучил основы организации производства, труда и управления на объекте информатизации, составил карту информационной системы организации.
Ознакомился с информационной системой безопасности предприятия, используемыми техническими средствами и программными продуктами, составил краткую характеристику информационной системы организации.
Изучил применяемые технологии и технические средства, используемые в целях обеспечения защиты информации на объекте.
Проводил выявление каналов утечки информации на объекте защиты, составление модели каналов утечки информации.
Изучил требования, предъявляемые к обеспечению информационной безопасности на объекте информатизации, разрабатывал политики безопасности в системах и сетях.
Характеристика учебной и профессиональной деятельности студента во время производственной практики Аттестуемый(ая) *продемонстрировал(а) / не продемонстрировал(а)* владение профессиональными и общими компетенциями

С целью овладения видом профессиональной деятельности «Обеспечение информационной безопасности систем мобильной связи» обучающимся были освоены общие и профессиональные компетенции:			
наименование ОК	Баллы (0-1) 0-не освоена, 1-освоена	наименование ПК	Баллы (0-1) 0-не освоена, 1-освоена
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.		ПК.3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи.	
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.		ПК.3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.		ПК.3.3. Обеспечивать безопасное администрирование систем и сетей.	
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 команде, эффективно общаться с коллегами, руководством, потребителями.			
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), 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.			
Общее количество баллов:_____ *Максимальное кол-во набранных баллов: 12* *Минимальное кол-во баллов: -0*			

Руководитель практики от предприятия:

_____ _____ _____

должность *подпись* *расшифровка*

Дата _____ _____ 20….. г.

МП

Приложение 5

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

СМОЛЕНСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ (ФИЛИАЛ) СПбГУТ
(СКТ(ф)СПбГУТ)

В Е Д О М О С Т Ь

20__/20__ учебный год

УП.03 Учебная практика
ПП.03 Производственная практика (по профилю специальности)
ПМ.03 Обеспечение информационной безопасности систем мобильной связи

Курс _____ группа _____

Специальность 11.02.08 Средства связи с подвижными объектами

Преподаватель _____
(фамилия, имя, отчество)

№№ пп	ФИО студента	Кол-во баллов по УП.03	Кол-во баллов по ПП.03	Кол-во баллов по отчету	Оценка результата КДЗ
……	……..				

Преподаватель _____ _____
(фамилия, имя, отчество)

Заведующий практикой _____ М.Д.Драницина

«___» _____ 20___ г.