СОГЛАСОВАНО
Начальник отдела защиты информации
Департамента цифрового развития
Смоленской области
_____ А.Н. Калугин
«31» 08 2023 г.

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

Комплект оценочных материалов для промежуточной аттестации
(другая форма аттестации - 7 семестр, дифференцированный зачет – 8 семестр)
по МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи
ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей
и систем связи
по специальности 11.02.15. Инфокоммуникационные сети и системы связи

Дифференцированный зачет является промежуточной формой контроля, подводит итог освоения МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи.

Результатом освоения программы МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи является овладение студентами профессиональных (ПК) и общих (ОК) компетенций:

ПК 3.1.	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
ПК 3.2.	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.
ПК 3.3.	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

Результатом освоения программы МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи являются освоенные умения и усвоенные знания.

В результате освоения МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи студент должен уметь:

У1 – классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

У2 - проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;

У3 – определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;

У4 - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;

У5 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;

У6 - выполнять тестирование систем с целью определения уровня защищенности;

У7 - определять оптимальные способы обеспечения информационной безопасности;

У8 проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;

У9 - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;

У10 - разрабатывать политику безопасности сетевых элементов и логических сетей;

У11 - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;

У12 - производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;

У13 - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

У14 - защищать базы данных при помощи специализированных программных продуктов;

У15 - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.

знать:

З1 – принципы построения информационно-коммуникационных сетей;

З2 - международные стандарты информационной безопасности для проводных и беспроводных сетей;

З3 - нормативно - правовые и законодательные акты в области информационной безопасности;

З4 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления и закрытия;

З5 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;

З6 - способы и методы обнаружения средств съёма информации в радиоканале;

З7 - классификацию угроз сетевой безопасности;

З8 - характерные особенности сетевых атак;

З9 - возможные способы несанкционированного доступа к системам связи;

З10 - правила проведения возможных проверок согласно нормативных документов ФСТЭК;

З11 - этапы определения конфиденциальности документов объекта защиты;

З12 - назначение, классификацию и принципы работы специализированного оборудования;

З13 - методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP. WPA и WPA2;

З14 - методы и средства защиты информации в телекоммуникациях от вредоносных программ;

З15 - технологии применения программных продуктов;

З16 - возможные способы, места установки и настройки программных продуктов;

З17 - методы и способы защиты информации, передаваемой по кабельным направляющим системам;

З18 - конфигурации защищаемых сетей;

З19 - алгоритмы работы тестовых программ;

З20 - средства защиты различных операционных систем и среды передачи информации;

З21 - способы и методы шифрования (кодирование и декодирование) информации.

Другая форма аттестации и дифференцированный зачёт являются промежуточными формами контроля, подводят итог освоения программы МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи.

Другая форма аттестации проводится в форме тестирования, дифференцированный зачёт по МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи проводится в форме тестирования. На промежуточную аттестацию выделяется по 2 часа (последнее занятие в семестре) из общего количества часов на МДК.03.01.

Тест содержит два блока: блок 1 для 7 семестра (в 1 блоке 85 тестовых позиций и 85 теоретических вопросов с кратким ответом, блок 2 для 8 семестра (70 тестовых позиций и 70 теоретических вопросов с кратким ответом).

Тест для 7 семестра содержит 30 вопросов (суммарно 20 тестовых позиций и 10 теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока заданий.

Время тестирования – 90 минут (по 2 минуте на каждый вопрос тестовых позиций и по 4 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 10 минут.

Тест для 8 семестра содержит 30 вопросов (суммарно 20 тестовых позиций и 10 теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока заданий.

Время тестирования – 90 минут (по 2 минуте на каждый вопрос тестовых позиций и по 4 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 10 минут.

Результаты другой формы аттестации и дифференцированного зачета определяются на основании итогового ответа с оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», вносятся в учебный журнал группы и объявляются в тот же день.

Критерии оценивания:

5 баллов - получают студенты, справившиеся с работой 100-90%;

4 балла - ставится в том случае, если верные ответы составляют 75%-89% от общего количества;

3 балла - соответствует работа, содержащая 55-74% правильных ответов;

2 балла - соответствует работа, содержащая менее 55% правильных ответов.

Шкала оценивания образовательных результатов:

Оценка	Критерии
«отлично»	Студент набрал 5 баллов
«хорошо»	Студент набрал 4 балла
«удовлетворительно»	Студент набрал 3 балла
«неудовлетворительно»	Студент набрал 0-2 балла

Тестовое задание для другой формы аттестации
по МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи
Блок 1(7 семестр)

1.	Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?	1.Доступность 2.Целостность 3.Конфиденциальность 4.Управляемость 5.Надежность
2.	Что понимается под атакой на информационную систему	1Любое действие, нарушающее безопасность информационной системы. 2.Действие или последовательность связанных между собой действий, использующих уязвимости данной информационной системы и приводящих к нарушению политики безопасности. 3.Использование ошибки в программном обеспечении. 4.Исключительно несанкционированный доступ в систему.
3.	Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется?	1.Мониторинг. 2.Аудит. 3.Управление ресурсами. 4.Администрирование.
4.	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.
5.	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.
6.	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.
7.	Что способна выявлять SIEM система?	1.Сетевые атаки во внутреннем и внешнем периметрах. 2.Вирусные эпидемии или отдельные вирусные заражения, не удаленные вирусы, бэкдоры и трояны. 3.Попытки несанкционированного доступа к

		конфиденциальной информации. 4.Фрод и мошенничество. 5.Ошибки и сбои в работе информационных систем. 6.Уязвимости. 7.Ошибки конфигураций в средствах защиты и информационных системах. 8.Все ответы верны.
8.	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.
9.	Что из перечисленного может быть участником аутентификационного процесса?	1.Пользователи. 2.Маршрутизаторы. 3.Межсетевые экраны. 4.Пароли.
10.	Сервис, который гарантирует, что информация получена из законного источника и получателем является тот, кто нужно, называется?	1.Аутентификацией. 2.Целостностью. 3.Конфиденциальностью. 4.Доступностью.
11.	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.
12.	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.
13.	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.
14.	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.
15.	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.
16.	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.
17.	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.
18.	Политиками по умолчанию для межсетевого экрана считаются?	1.Запретить весь входящий трафик, который явно не разрешен. 2.Разрешить весь входящий трафик, который явно не запрещен. 3.Разрешить весь исходящий трафик, который явно не запрещен. 4.Запретить весь исходящий трафик, который явно не разрешен.
19.	Межсетевого экрана какого класса не существует?	1.Экранирующий маршрутизатор. 2.Экранирующий коммутатор. 3.Экранирующий транспорт. 4.Экранирующий шлюз.
20.	Какую аутентификацию рекомендуется использовать при удаленном доступе?	1.Однофакторную. 2.Двухфакторную. 3.Трехфакторную.
21.	Какие записи должны вестись при аудите?	1.Вход/выход пользователей. 2.Неудачные попытки входа. 3.Все системные события 4.Зависит от уровня аудита.
22.	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.
23.	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.
24.	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.
25.	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.
26.	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.
27.	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.
28.	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.
29.	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
30.	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
31.	При полномочной политике безопасности совокупность меток с одинаковыми значениями образует?	1.Уровень безопасности. 2.Область равной критичности. 3.Область равного доступа. 4.Уровень доступности.
32.	В системах управления доступом субъектом может быть?	1.Пользователь. 2.Аппаратное устройство. 3.Процесс ОС. 4.Прикладная система. 5.Все ответы верны.
33.	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.

34.	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).
35.	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.
36.	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.
37.	Каковы преимущества пользовательских VPN?	1.Сотрудники, находящиеся в командировке могут подключаться к сети компании. 2.Сотрудники могут работать из дома. 3.Преимуществ нет.
38.	Некоторая уникальная информация, позволяющая различать пользователей называется?	1.Идентификатор (логин). 2.Пароль. 3.Учетная запись. 4.Ключ.
39.	Секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется?	1.Идентификатор (логин). 2.Пароль. 3.Учетная запись. 4.Ключ.
40.	Совокупность идентификатора и пароля пользователя называется?	1.Логин пользователя. 2.Учетная запись пользователя. 3.Ключ пользователя.
41.	Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является?	1.Идентификацией пользователя. 2.Аутентификацией пользователя. 3.Опознанием пользователя. 4.Созданием учетной записи пользователя.
42.	Проверка принадлежности пользователю предъявленного им идентификатора называется?	1.Идентификацией пользователя. 2.Аутентификацией пользователя. 3.Регистрацией пользователя. 4.Созданием учетной записи пользователя.
43.	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.

44.	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.
45.	Невозможность получения сервиса законным пользователем называется?	1.DoS-атакой. 2.Replay-атакой. 3.Пассивной атакой. 4.Атакой «man-in-the-middle».
46.	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.
47.	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.
48.	Где лучше размещать VPN сервер?	1.В отдельной DMZ. 2.В DMZ интернета, вместе с остальными серверами. 3.Во внутренней сети компании.
49.	Какой должна быть система аутентификации, использующаяся в VPN?	1.Однофакторной. 2.Двухфакторной. 3.Трехфакторной. 4.Четырехфакторной.
50.	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.
51.	Какое средство аутентификации рекомендуется использовать в VPN?	1.Смарт-карту и пароль. 2.Только смарт-карту. 3.Только пароль. 4.Биометрическую идентификацию.
52.	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.
53.	Какие из указанных контрмер позволяют компенсировать физические уязвимости?	1.Межсетевые экраны. 2.Устройства считывания смарт-карт при входе в помещения. 3.Охрана. 4.Шифрование.
54.	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.
55.	Наличие какого элемента характерно для всех архитектур DMZ?	1.Почтовый сервер. 2.DNS. 3.NTP. 4.Межсетевой экран.

56.	Как расшифровывается аббревиатура DMZ?	1.Демилитаризованная зона. 2.Зона управления данными. 3.Зона ежедневного управления. 4.Зона поддержки данных.
57.	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.
58.	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.
59.	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.
60.	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.
61.	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.
62.	Как называется сетевая атака, целью которой является поиск открытых портов работающих в сети устройств, определение типа и версии ОС и ПО, контролирующего открытый порт?	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.
63.	Что следует определить при анализе производительности межсетевого экрана?	1.Какую пропускную способность, максимальное количество одновременно открытых соединений, соединений в секунду может обеспечивать межсетевой экран. 2.Возможна ли балансировка нагрузки и резервирование для гарантирования высокой отказоустойчивости. 3.Что является более предпочтительным – аппаратный или программный межсетевой экран. 4.Какое количество портов существует на выбранном экземпляре межсетевого экрана.
64.	Что следует рассмотреть при внедрении персональных межсетевых экранов и межсетевых экранов для	1.Удовлетворяют ли рабочие станции и сервера минимальным системным требованиям, которые необходимы для функционирования межсетевого

	хостов?	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.
65.	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.
66.	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.
67.	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.
68	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.
69.	Какие устройства могут выполнять функции NAT?	1.Маршрутизаторы. 2.Межсетевые экраны. 3.Почтовые сервера. 4.DNS сервера.
70.	В системах управления доступом объектом доступа может быть?	1.Файл. 2.Любой сетевой ресурс, к которому субъект хочет получить доступ. 3.Аппаратное устройство. 4.Прикладная система. 5.Все ответы верны.
71.	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.
72.	Каковы общие свойства систем анализа уязвимостей и систем	1.И те, и другие следят за конкретными симптомами проникновения и другими нарушениями политики

	обнаружения вторжений?	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.
73.	Что необходимо обеспечить при управлении конфигурациями?	1.Регулярное изменение правил фильтрации. 2.Регулярное обновление ПО. 3.Управление изменениями. 4.Оценка состояния сетевой безопасности.
74.	Документ, устанавливающий требования, спецификации, руководящие принципы или характеристики, в соответствии с которыми могут использоваться материалы, продукты, процессы и услуги, которые подходят для этих целей называется?	1. Нормативно-методический документ. 2.Стандарт. 3.Руководящий документ. 4. Нормативно правовой акт.
75.	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.
76.	Под унифицированным управлением угрозами (Unified Threat Management – UTM) понимают?	1.Централизованное управление несколькими сетевыми устройствами. 2.Создание базы данных потенциальных угроз. 3.Создание базы данных точек входа в сеть. 4.Централизованное управление всеми межсетевыми экранами.
77.	Что включает в себя типовая 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.
78.	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.
79.	Для каких целей устанавливается IDS?	1.Обнаружение атак 2.Предотвращение атак 3.Обнаружение нарушений политики 4.Повышение надежности системы.
80.	Межсетевые экраны какого типа 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»
81.	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.
82.	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.
83.	Межсетевые экраны какого типа 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»
84.	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.
85.	Межсетевые экраны какого типа 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»

Вопросы задания открытого типа для другой формы аттестации
по МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи
Блок 1(7 семестр)

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

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

3.Как называется процедура 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 выделено ФСТЭК?

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, 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?

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

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.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?

42.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?

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

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

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

46.Однократный ввод учетных данных для доступа к нескольким системам/приложениям, - это?

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

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

49. 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?

50.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?

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

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

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

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

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

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

57.В каком подходе к обнаружению атак системы обнаружения атак (СОА) осуществляют

поиск шаблонов известных атак в сетевом трафике или высокоуровневых данных?

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

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

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

61.Назовите два основных этапа работ по анализу защищенности, проводимых по отношению к периметру корпоративной сети?

62. 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?

63. 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?

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

65.Устройство или программное обеспечение для перехвата данных, вводимых с клавиатуры, которое распознаёт нажатия кнопок, скрыто сохраняет и передает информацию злоумышленнику - это?

66.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?

67.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?

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

69. 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?

70. Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа, - это?

71.Какая учетная запись имеет больше прав, чем стандартная учетная запись, однако объем прав таких записей может существенно различаться в зависимости от организации, должностных обязанностей и используемых технологий?

72.Процесс сбора и анализа информации об ИС и реализованных организационно-технических мерах защиты для качественной или количественной оценки уровня ее защищенности и/или установления соответствия требованиям нормативных документов, - это?

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

74. 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?

75. 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?

76.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?

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

78. Файлы с записями о событиях в хронологическом порядке называют?

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

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

81. Какую функцию выполняет межсетевой экран?

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

83. Для чего необходимо ограничивать доступ во внутреннюю сеть со стороны общедоступной сети за счет применения фильтров и средств аутентификации?

84. На какие группы можно разделить все межсетевые экраны по способу их реализации?

85. 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?

Тестовое задание закрытого типа для дифференцированного зачета
по МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи
Блок 2 (8 семестр)

1.	Что входит в комплексную систему защиты информации?	1. Средства управления учетными записями. 2. Средства управления событиями. 3. Средства защищенного доступа. 4. Средства контроля защищенности. 5. Средства разделения физической сети на несколько логических сетей.
2.	Что относят к физическим средствам защиты?	1.Стены. 2. Заграждения. 3. Решетки. 4. Межсетевые экраны 5. Ударо- и взрывостойкое остекление. 6. Устройства хранения. 7. Замки (механические, электрические, электромеханические, гидравлические)
3.	Какие задачи решает система физической защиты?	1. Предупреждения несанкционированного доступа, нерегламентированных воздействий. 2. Задержки нарушителей, их выявления на объекте. 3. Реагирования сотрудников службы безопасности. 4. Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 5. Обеспечение целостости программно-аппаратной среды
4.	Какие бывают объекты защиты при обеспечении информационной безопасности?	1. Информация. 2. Ресурсные объекты. 3. Физические объекты. 4. Пользовательские объекты. 5. Устройства хранения. 6. Устройства передачи данных.
5.	Какие компоненты входят в комплекс защиты охраняемых объектов?	1. Сигнализация 2. Охрана 3. Датчики 4. Телевизионная система 5. Устройства несанкционированного доступа, нерегламентированных воздействий. 6. Устройства обеспечения целостости программно-

		аппаратной среды.
6.	Какой документ определяет требования и порядок создания системы защиты персональных данных?	1.Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных". 2.Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". 3.Все ответы верны.
7.	Какие бывают системы защиты?	1.Система защиты от угроз несанкционированного доступа. 2. Система защиты от угроз вредоносного кода. 3. Система межсетевого экранирования и защиты каналов связи. 4. Система анализа защищенности. 5.Система обнаружения вторжений. 6. Система нерегламентированных воздействий. 7. Система защиты носителей информации для идентификации и аутентификации пользователей.
8.	Решение каких задач обеспечивает система защиты информации от угроз несанкционированного доступа?	1.Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 2.Обеспечение функций регистрации и учета событий безопасности. 3.Обеспечение неизменности (целостости) программно-аппаратной среды применяемых программных и программно-технических средств. 4. Задержка нарушителей, их выявление на объекте. 5. Реагирование сотрудников службы безопасности.
9.	Что из перечисленного входит в состав системы защиты от несанкционированного доступа?	1.Средства централизованного управления средствами защиты от несанкционированного доступа; 2.Сертифицированные средства защиты от несанкционированного доступа; 3.Встроенные в системное программное обеспечение средства идентификации, аутентификации, авторизации, мониторинга событий и контроля целостности; 4.Средства удаленного администрирования автоматизированных рабочих мест и серверов, входящих в состав информационной системы; 5.Средства резервного копирования и восстановления конфигураций и других параметров настроек применяемых средств защиты от несанкционированного доступа. 6. Все ответы верны.
10.	Какие существуют виды угроз информационной безопасности (внешние и внутренние)?	1. Несанкционированный доступ 2. Угроза утечки информации 3. Мошенничество 4. Кибервойны и кибертерроризм 5. Угроза аутентификации пользователей. 6. Верификация.
11.	Сколько существует групп методов обеспечения безопасности?	1. Технические. 2. Административные. 3. Правовые. 4. Физические. 5. Превентивные. 6. Восстановительные.
12.	Какие меры включает в себя система защиты персональных данных?	1.Установление ограничений по доступу персонала к личным сведениям; 2.Выбор ответственного за безопасность ПДн лица; 3.Составление и утверждение локальных документов; 4.Информирование персонала о требованиях по работе с

		цифровыми или бумажными персональными данными; 5. Задержка нарушителей, их выявление на объекте защиты; 6. Все ответы верны.
13.	Что из перечисленного является методами защиты информации от случайных информационных угроз ПДн?	1.Использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей; 2.Использование средств антивирусной защиты; 3.Централизованное управление системой защиты персональных данных информационной системы; 4.Средства удаленного администрирования автоматизированных рабочих мест и серверов, входящих в состав информационной системы; 5.Средства резервного копирования и восстановления конфигураций средств защиты от несанкционированного доступа.
14.	Какие методы используются для обеспечения информационной защиты данных, хранящихся и передающихся техническими средствами?	1.Аутентификация; 2.Регламентирование доступа к объектам; 3.Шифрующая система файлов; 4.Ключи; 5.Безопасные соединения; 6.Выбор ответственного за безопасность лица; 2.Использование средств антивирусной защиты;
15.	Как можно защищать корпоративную информацию?	1. Использовать удаленного администрирования автоматизированных рабочих мест и серверов, входящих в состав корпоративной системы 2. Установить четкие правила и регламенты работы с информацией, назначить наказания за их нарушение. 3. Закрыть информацию от несанкционированного доступа с помощью технических инструментов: аппаратуры или специального программного обеспечения.
16.	Какие из перечисленных средств относятся к средствам обнаружения угроз?	1.Охранная сигнализация. 2.Охранное телевидение. 3. Ударо- и взрывостойкое остекление. 4. Устройства хранения. 5. Электромеханические и гидравлические замки.
17.	Какие средства безопасности используются для защиты данных в информационных системах?	1.Персонализация. 2.Авторизация. 3.Верификация. 4.Ограничение доступа к активам пользователей. 5.Шифрование. 6. Все ответы верны.
18.	Что из перечисленного относится к инженерным средствам защиты?	1.Аутентификация. 2. Средства удаленного администрирования автоматизированных рабочих мест и серверов. 3.Ограждение периметра ПС и внутренних зон ограниченного доступа. 4.Контрольно-пропускные пункты (КПП) с соответствующим досмотровым оборудованием. 5.Въездные ворота, калитки, шлагбаумы.
19.	Какие существуют технические каналы утечки информации?	1.Визуально-оптические каналы утечки информации. 2.Акустические каналы утечки информации.3.Электромагнитные каналы утечки информации (или каналы утечки информации по ПЭМИН). 4.Материально-вещественные каналы утечки информации. 5. Визуально-вещественные каналы утечки информации.

		6. Все ответы верны.
20.	Как классифицируются технические каналы акустической (речевой) утечки информации в зависимости от физической природы возникновения информационных сигналов, среды их распространения?	1. Прямые акустические (воздушные). 2. Акустовибрационные. 3. Акустооптические (лазерные). 4. Акустоэлектрические. 5. Акустовизуальные. 6. Все ответы верны.
21.	Какие причины имеют место при бесконтрольном распространении важных сведений за пределы компании?	1.Недостаточный уровень компетенции сотрудников, которые работают в сфере защиты информации, их недопонимание важности сохранности данных, а также безответственное отношение к своей деятельности. 2.Использование нелицензионного ПО, или не прошедших аттестацию программ по защите клиентов и личных данных. 3. Правильно организованный контроль над средствами защиты важных сведений. 4.Высокая текучка кадров, задействованных в данной сфере деятельности.
22.	Что из перечисленного является косвенными каналами утечки информации?	1.Пропажа, кража или утеря информационного накопителя, исследование не удаленной корзины. 2.Прослушивание, дистанционные снимки. 3.Перехват электромагнитных устройств. 4. Утечка данных из-за несоблюдения режима коммерческой тайны. 5.Непосредственное копирование данных.
23.	Что из перечисленного является прямыми каналами утечки информации?	1. Прослушивание, дистанционные снимки. 2. Перехват электромагнитных устройств. 3. Человеческий фактор. 4. Утечка данных из-за несоблюдения режима коммерческой тайны. 5. Непосредственное копирование данных.
24.	При каких режимах обработки информации средствами вычислительной техники возникают побочные электромагнитные излучения?	1. Вывод информации на экран монитора. 2. Ввод данных с клавиатуры. 3. Запись информации на накопители. 4. Чтение информации с накопителей. 5. Передача данных в каналы связи. 6. Вывод данных на периферийные печатные устройства - принтеры, плоттеры. 7. Запись данных от сканера на магнитный носитель. 8. Все ответы верны.
25.	Где могут возникнуть наводки информативных сигналов?	1. В линиях электропитания ТСОИ. 2. В линиях электропитания и соединительных линиях ВТСС. 3. В цепях заземления ТСОИ и ВТСС. 4. В посторонних проводниках (неметаллических трубах, пластмассовых конструкциях). 5. Все ответы верны.
26.	Как создаются возможные каналы утечки информации?	1.Низкочастотными электромагнитными полями, которые возникают во время работ ТСПИ и ВТСС. 2.Во время влияния на ТСПИ и ВТСС электрических, магнитных и акустических полей. 3. При возникновении паразитной высокочастотной (ВЧ) генерации. 4. При прохождении информативных (опасных) сигналов в цепи электропитания. 5. При взаимном влиянии цепей. 6. При прохождении информативных (опасных) сигналов в цепи заземления; 7.При паразитной модуляции сигнала. 8. Вследствие ошибочных коммутаций и несанкционированных действий.

		9. Все ответы верны.
27.	Что из перечисленного относится к электромагнитным каналам утечки информации (КУИ)?	1. Перехват побочных электромагнитных излучений (ПЭМИ) элементов ТСПИ. 2. Перехват ПЭМИ на частотах работы высокочастотных (ВЧ) генераторов в ТСПИ и ВТСС. 3. Перехват ПЭМИ на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ. 4. Съем информационных сигналов с линий электропитания ТСПИ. 5. Съем информационных сигналов с цепей заземления ТСПИ и ВТСС.
28.	Что из перечисленного относится к электрическим каналам утечки информации (КУИ)?	1.Съем наводок ПЭМИ ТСПИ с соединительных линий ВТСС и посторонних проводников. 2. Съем информационных сигналов с линий электропитания ТСПИ. 3. Съем информационных сигналов с цепей заземления ТСПИ и ВТСС. 4. Съем информации путем установки в ТСПИ электронных устройств перехвата информации. 5. Перехват побочных электромагнитных излучений (ПЭМИ) элементов ТСПИ. 6. Перехват ПЭМИ на частотах работы высокочастотных (ВЧ) генераторов в ТСПИ и ВТСС.
29.	Что из перечисленного является целями и задачами технической защиты информации?	1.Предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения. 2.Защита носителей информации от уничтожения в результате различных природных и техногенных воздействий. 3.Предотвращение утечки информации по различным техническим каналам. 4. Использование лицензионного ПО, или прошедших аттестацию программ по защите клиентов и личных данных. 5. Систематическое обновление программного обеспечения.
30.	Что из перечисленного относится к ТСПИ и ВТСС?	1. Задающие генераторы. 2. Генераторы тактовой частоты. 3. Генераторы стирания и подмагничивания магнитофонов, 4. Гетеродины радиоприемных и телевизионных устройств. 5. Все ответы верны.
31.	Какие основные средства включает в себя система видеоконтроля?	1. Передающие телевизионные камеры. 2. Устройства отображения видеоинформации – мониторы. 3. Устройства обработки видеоинформации (коммутаторы, квадраторы, мультиплексоры). 4. Устройства регистрации информации (бытовые и специальные видеомагнитофоны); 5. Кабели, обеспечивающие электрические связи элементов системы видеонаблюдения. 6. Устройства тревожной звуковой и световой сигнализации. 7. Средства пожаротушения.
32.	Какими способами можно избежать утечки персональных данных?	1.Установка антивирусных программ. 2. Использование межсетевого экрана. 3. Повышение квалификации пользователей. 4. Строгое разграничение доступа персонала к базам данных и интернету. 5. Систематическое обновление программного

		обеспечения. 6. Все ответы верны.
33.	Что из перечисленного является примером прямого канала утечки данных?	1. Пропажа, кража информационного накопителя. 2. Прослушивание, дистанционные снимки. 3. Перехват электромагнитных устройств. 4. Работа инсайдеров.
34.	Как бороться с утечкой персональных данных?	1. Использовать надежные пароли и настроить многофакторную аутентификацию. 2. Своевременно обновлять программное обеспечение. 3. Регулярно создавать резервные копии данных. 4. Обновить адресную книгу электронной почты. 5. Стараться не заходить на незащищенные веб-сайты. 6.Все ответы верны.
35.	Какими способами обеспечивается защита информации от утечки по электромагнитным каналам?	1.Экранирование элементов и узлов оборудования. 2.Фильтрация в цепях заземления и питания. 3.Ослабление связей между элементами (индуктивной, электромагнитной). 4. Установка в ТСПИ электронных устройств перехвата информации.
36.	Какие каналы утечки информации выявляются в процессе поисковых мероприятий?	1.Обрабатываемые ТСПИ. 2.Речевой информации. 3.Визуально-графической информации. 4.Видовой информации. 5.Цифровой информации.
37.	Какими способами в ходе специальной проверки, выполняемой с применением пассивных и активных поисковых средств, осуществляется выявление закладных устройств?	1.Контроль радиоспектра и побочных электромагнитных излучений ТСПИ. 2.Выявление с помощью индикаторов электромагнитного поля, интерсепторов, частотомеров, сканеров или программно-аппаратных комплексов негласно установленных подслушивающих приборов. 3.Специальная проверка выделенных помещений, ТСПИ и ВТСС с использованием нелинейных локаторов и мобильных рентгеновских установок. 4.Все ответы верны.
38.	Что из перечисленного относят к пассивным техническим способам защиты?	1.Установка комплексных систем защиты от несанкционированнного доступа на ТСПИ и кабельные линии связи. 2.Экранирование ВП, ТСПИ и отходящих от них соединительных линий. 3.Заземление ТСПИ и экранов соединительных линий приборов. 4.Звуко- и виброизоляция ВП и механических узлов ТСПИ. 5.Разрушающее воздействие на средства съема сигналами большой мощности (тепловое разрушение электронных устройств). 6.Установка систем гарантированного уничтожения информации.
39.	Что из перечисленного относят к пассивным техническим способам защиты?	1.Встраивание в ВТСС, обладающие “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров. 2.Использование специальных конструкций оконных блоков, специальных пленок, жалюзи и штор. 3.Установка автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ. 4.Монтаж в цепях электропитания ТСПИ, а также в электросетях ВП помехоподавляющих фильтров. 2.Акустическое и вибрационное зашумление строительных конструкций. 3.СВЧ - воздействие на микрофонные цепи (подавления

		диктофонов устройствами направленного высокочастотного радиоизлучения).
40.	Какими методами осуществляется активное воздействие на каналы утечки информации?	1.Пространственное электромагнитное зашумление ЗУ и ПЭМИН ТСПИ. 2.Акустическое и вибрационное зашумление строительных конструкций. 3.СВЧ - воздействие на микрофонные цепи (подавления диктофонов устройствами направленного высокочастотного радиоизлучения). 4.Зашумление каналов передачи данных. 5.Встраивание в ВТСС, обладающие “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров. 6.Использование специальных конструкций оконных блоков, специальных пленок, жалюзи и штор.
41.	Какими способами осуществляется активное воздействие на каналы утечки информации?	1.Зашумления силовой сети и цепей заземления. 2.Разрушающее воздействие на средства съема сигналами большой мощности (тепловое разрушение электронных устройств). 3.Установка систем гарантированного уничтожения информации. 4.Шифрование информации, передаваемой по каналам связи. 5.Установка автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ. 6.Монтаж в цепях электропитания ТСПИ, а также в электросетях ВП помехоподавляющих фильтров.
42.	Какие методы защиты информации могут быть использованы для предотвращения несанкционированного доступа?	1.Пароли для авторизации во время работы. 2.Модули доверенной загрузки. 3.Криптографические средства шифрования информации для ее передачи и хранения. 4.Средства предотвращения сетевых атак (межсетевой экран, антивирус, прокси-сервер). 5.Все ответы верны.
43.	Какие компоненты включает в себя комплекс радиолокационной системы?	1.Система периметрального наблюдения, состоящая из камер и тепловизоров. 2.Инфракрасные и вибрационные извещатели. 3.Радиолокатор. 4.Рабочее операторское место. 5. Модули доверенной загрузки. 6. Система гарантированного уничтожения информации.
44.	Что из перечисленного является основными закономерностями распространения радиоволн, которые позволяют обнаруживать объекты и измерять координаты и параметры их движения?	1.Постоянство скорости и прямолинейность распространения радиоволн в однородной среде. 2.Способность радиоволн отражаться от различных областей пространства, электрические или магнитные параметры которых отличаются от аналогичных параметров среды распространения. 3. Изменение частоты принимаемого сигнала по отношению к частоте излученного сигнала при относительном движении источника излучения и приемника радиолокационного сигнала. 4. Изменение скорости принимаемого сигнала.
45.	Какие виды средств защиты информации должны содержаться в информационных системах общего пользования?	1.СЗИ от неправомерных действий (в том числе средства криптографической защиты информации). 2.Средства обнаружения вредоносных программ (в том числе антивирусные средства). 3.Средства контроля доступа к информации (в том числе средства обнаружения компьютерных атак). 4.Средства фильтрации и блокирования сетевого трафика (в том числе средства межсетевого

		экранирования). 5. Все, перечисленное в остальных пунктах.
46.	Какие виды средств криптографической защиты информации различают по ГОСТ Р 50922-2006?	1.Средства шифрования. 2.Средства имитозащиты. 3.Средства электронной подписи. 4.Средства кодирования. 5.Средства изготовления ключевых документов. 6.Ключевые документы. 7.Аппаратные шифровальные (криптографические) средства. 8.Программные шифровальные (криптографические) средства. 9.Программно-аппаратные шифровальные (криптографические) средства. 10. Все, перечисленное в остальных пунктах.
47.	Является ли лицензируемым видом деятельности разработка, изготовление и распространение средств защиты информации, реализующих алгоритмы криптографического преобразования информации?	1.Да, является. 2.Нет, не является.
48.	Какие средства криптографической защиты обеспечивают создание электронной цифровой подписи с использованием закрытого ключа, подтверждение с использованием открытого ключа подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
49.	Какие средства криптографической защиты информации обеспечивают возможность разграничения доступа к ней?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
50.	Какие средства шифрования обеспечивают создание ключевых документов?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
51.	Какие СЗИ обеспечивают защиту от навязывания ложной информации, возможность обнаружения изменений информации с помощью реализованных в СЗИ криптографических механизмов?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты 5.Средства шифрования.
52.	Средства шифрования, в которых часть криптопреобразований осуществляется с использованием ручных операций или автоматизированных средств, предназначенных для выполнения таких операций, - это?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
53.	Как называют электронные документы, содержащие ключевую информацию, необходимую для выполнения криптографических преобразований с помощью средств шифрования?	1.Шифрованные документы. 2.Кодовые документы. 3.Ключевые документы. 4.Подлинные документы.
54.	Сколько классов криптографических	1.Шесть классов.

	средств защиты информации определено ФСБ России?	2.Пять классов. 3.Семь классов. 4.Четыре класса.
55.	К основным особенностям СЗИ этого класса относится их возможность противостоять атакам, проводимым из-за пределов контролируемой зоны?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
56.	К основным особенностям СЗИ этого класса относится их возможность противостоять атакам, блокируемым средствами класса КС1, а также атакам, проводимым в пределах контролируемой зоны?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
57.	В случае возможности противостоять атакам при наличии физического доступа к средствам вычислительной техники с установленными криптографическими СЗИ говорят о соответствии таких средств какому классу?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
58.	Если криптографическое СЗИ противостоит атакам, при создании которых участвовали специалисты в области разработки и анализа указанных средств, в том числе научно-исследовательские центры, была возможность проведения лабораторных исследований средств защиты, то речь идет о соответствии какому классу?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
59.	Если к разработке способов атак привлекались специалисты в области использования НДВ системного программного обеспечения, была доступна соответствующая конструкторская документация и был доступ к любым аппаратным компонентам криптографических СЗИ, то защиту от таких атак могут обеспечивать средства какого класса?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
60.	Какие бывают наземные РЛС?	1.Подвижные. 2.Стационарные. 3.Надгоризонтные. 4.Загоризонтные. 5.Подповерхностные. 6.Надповерхностные
61.	Какой метод использует для своей работы индикатор поля?	1.Метод широкополосного прямого детектирования. 2.Метод узкополосного прямого детектирования. 3.Метод широкополосного обратного детектирования. 4.Метод узкополосного обратного детектирования.
62.	Что из перечисленного относится к средствам защиты акустической речевой информации?	1.Системы оптической защиты. 2.Средства защиты слаботочных линий. 3.Средства защиты от несанкционированного применения сотовых телефонов, диктофонов и радиопередатчиков. 4.Электромагнитные подавители сотовых телефонов.
63	Что из перечисленного является основными организационными мероприятиями по защите речевой (акустической) информации,	1.Выбор помещений для ведения конфиденциальных переговоров (защищаемых помещений). 2. Категорирование защищаемых помещений. 3. Использование в защищаемых помещениях

	составляющей коммерческую тайну?	сертифицированных ВТСС. 4. Установление контролируемой зоны вокруг защищаемых помещений. 5. Демонтаж в защищаемых помещениях незадействованных ВТСС, их соединительных линий и посторонних проводников. 6. Организация режима и контроля доступа в защищаемые помещения. 7. Все ответы верны.
64	Какие из перечисленных решений могут быть интегрированы для организации единой системы защиты от потенциальных кибератак?	1.Безопасность приложений 2.Безопасность в облаке 3.Безопасность Интернета вещей 4.Безопасность критически важной инфраструктуры 5.Сетевая безопасность 6.Безопасность оконечных устройств 7.Все ответы верны.
65.	Какие из перечисленных решений могут быть интегрированы для организации единой системы защиты от потенциальных кибератак?	1.Предотвращение потери данных 2.Управление идентификацией и доступом (IAM) 3.Управление информационной безопасностью и событиями безопасности (SIEM) 4.Обучение для повышения осведомленности о кибербезопасности. 5.Информационная безопасность 6.Все ответы верны.
66.	Какие бывают типы угроз кибербезопасности?	1.Атаки на основе социальной инженерии. 2.Атаки при помощи вредоносного ПО. 3.Атаки на Интернет вещей (IoT). 4.Постоянная серьезная угроза (advanced persistent threat, APT). 5.Атаки типа «отказ в обслуживании» (DoS). 6.Все ответы верны.
67.	В чем разница между информационной безопасностью и кибербезопасностью?	1.Информационная безопасность направлена на защиту всех данных организации независимо от их типа (цифровые или аналоговые) и места хранения. 2.Кибербезопасность направлена на защиту цифровых данных от компрометации или атак. 3.Кибербезопасность направлена на защиту всех данных организации независимо от их типа (цифровые или аналоговые) от компрометации или атак. 4.Информационная безопасность направлена на защиту цифровых данных от компрометации или атак.
68.	Что представляют собой угрозы типа APT (advanced persistent threat)?	1.Программы-вымогатели, которые получают доступ к файлам или системам и блокируют их для получения выкупа. 2.Многоступенчатые атаки, в ходе которых хакеры проникают в сеть незамеченными и остаются в ней в течение длительного времени, чтобы получить доступ к конфиденциальным данным или нарушить работу критически важных служб. 3.Практика манипулирования людьми с целью заставить их раскрыть чувствительную конфиденциальную информацию для получения денежной выгоды или доступа к данным.
69.	Что из перечисленного является организационными методами защиты информации?	1.Разработка и внедрение регламентов по обработке сведений внутри организации. 2.Проведение инструктажа персонала по основам кибербезопасности и правилам работы с информацией. 3.Регулярное создание бэкапов наиболее важных и ценных информационных массивов. 4.Выполнение резервирования, дублирования вспомогательных компонентов информационной

		системы, которые связаны с хранением информации.
70.	Что из перечисленного является организационными методами защиты информации?	1.Создание защиты информационных ресурсов от ЧС. 2.Использование ПО, отвечающего за управление доступом к информации, ведение мониторинга, предотвращение утечек информации. 3.Установление зон ответственности. Руководитель назначает конкретных персон, ответственных за исполнение правил и норм информационной безопасности. 4.Разработка плана по восстановлению информации при чрезвычайных ситуациях.

Вопросы задания открытого типа для дифференцированного зачета
по МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи
Блок 2(8 семестр)

1.Задача обеспечения доступности внешних ресурсов компании всегда была актуальна для организаций, продающих свои товары и услуги через сайты. Недоступность сайта может привести и к финансовым потерям - в виде недополученной прибыли или снижения клиентопотока, - и к имиджевым. Самым эффективным вредоносным инструментом, с помощью которого злоумышленники могут вызвать подобную недоступность, являются атаки, во время которых генерируются миллионы запросов, «подвешивающих» серверы и приложения. Как называют эти атаки?

2.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?

3.Какой криптографический протокол обеспечивает защищённую передачу данных между узлами в сети Интернет?

4.Каковы основные функции протокола TLS?

5.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?

6. 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)?

7.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?

8.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?

9.Какие средства безопасности предназначены для анализа защищенности информации в корпоративных сетях и могут выполнять функции проверки сетевых устройств; проверки возможности осуществления атак типа "Denial of Service", "Spoofing"; проверки паролей; проверки межсетевых экранов; проверки удаленных сервисов; проверки DNS; проверки учетных

записей ОС; проверки установленных patch'ей системы безопасности ОС?

10.При сравнении межсетевых экранов, помимо цены и наличия сертификата ФСТЭК, необходимо обращать внимание на функциональную составляющую и выбирать не просто межсетевые экраны, а полноценные сетевые шлюзы безопасности, состоящие из шлюзового антивируса; блокировки сайтов по их содержимому, категории или конкретному адресу; VPN; мониторинга сетевой активности; управления пропускной способностью интернет-доступа. Как называются такие решения?

11.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)?

12.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?

13.Какую технологию используют для объединения компьютерных сетей организации, географически удаленных друг от друга, где заложен принцип шифрования данных, передаваемых через публичную сеть интернет, другими словами, - никто, кроме участников, не сможет открыть эти данные и воспользоваться ими?

14. 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)?

15. 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)?

16. К какому виду программно-технических средств обеспечения информационной безопасности относят шифрование и цифровую подпись?

17. К какому виду программно-технических способов и средств обеспечения информационной безопасности относят пароль; ключ доступа (физический или электронный); сертификат; биометрию?

18. К какому виду программно-технических способов и средств обеспечения информационной безопасности относят источники бесперебойного питания; резервирование нагрузки; генераторы напряжения.

19.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?

20.Технология идентификации, основанная на использовании радиочастотного электромагнитного излучения, называется?

21.Технология беспроводной высокочастотной связи малого радиуса действия (до 10 см), позволяющая осуществлять бесконтактный обмен данными между устройствами, расположенными на небольших расстояниях, называется?

22.Наносимая в виде штрихов закодированная информация о некоторых наиболее существенных параметрах объекта, считываемая при помощи специальных устройств, называется?

23.Двумерный штрихкод, в котором кодируется информация, состоящая из символов (включая кириллицу, цифры и спецсимволы), называется?

24.Идентификация человека по уникальным биологическим признакам называется?

25.На какие две группы делятся методы биометрической идентификации?

26.Какие методы биометрической идентификации основываются на уникальной физиологической характеристике человека, данной ему от рождения и неотъемлемой от него?

27.В основе какого метода биометрической идентификации используется уникальный для каждого человека рисунок папиллярных узоров на пальцах, т.е. отпечаток, полученный с помощью специального сканера, который преобразуется в цифровой код (свертку), и сравнивается с ранее введенным эталоном?

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

с помощью специального устройства, состоящего из камеры и нескольких подсвечивающих диодов (включаясь по очереди, они дают разные проекции ладони), строится трехмерный образ кисти руки, по которому формируется свертка и распознается человек?

29.При каком методе биометрической идентификации с помощью инфракрасной камеры считывается рисунок вен на лицевой стороне ладони или кисти руки; полученная картинка обрабатывается, и по схеме расположения вен формируется цифровая свертка.

30.При каком способе биометрической идентификации используется рисунок кровеносных сосудов глазного дна, для того чтобы этот рисунок стал виден – человеку нужно посмотреть на удаленную световую точку, и таким образом подсвеченное глазное дно сканируется специальной камерой?

31.При каком способе биометрической идентификации достаточно портативной камеры со специализированным программным обеспечением, позволяющим захватывать изображение части лица, из которого выделяется изображение глаза и рисунок, по которому строится цифровой код для идентификации человека?

32.При каком методе биометрической идентификации строится трехмерный образ лица человека, - на лице выделяются контуры бровей, глаз, носа, губ, вычисляется расстояние между ними и строится не просто образ, а еще множество его вариантов на случаи поворота лица, наклона, изменения выражения?

33. В основе какого метода биометрической идентификации лежит уникальность распределения на лице артерий, снабжающих кровью кожу, которые выделяют тепло и используются специальные камеры инфракрасного диапазона?

34.Какие методы биометрической идентификации основываются на поведенческой характеристике человека, построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия?

35. При каком методе биометрической идентификации не нужно никакого специального оборудования, кроме стандартной клавиатуры, и основной характеристикой, по которой строится свертка для идентификации является динамика набора кодового слова?

36.Какие системы кодируют в цифровом виде и хранят индивидуальные характеристики, позволяющие практически безошибочно идентифицировать любой индивид?

37.Как называют пластиковые карты со встроенной микросхемой, в большинстве случаев содержащие микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти?

38.Какое компактное USB-устройство, предназначено для безопасной аутентификации пользователей, защищенного хранения ключей шифрования и ключей электронной подписи, а также цифровых сертификатов?

39.Какое USB-устройство обеспечивает двухфакторную аутентификацию в компьютерных системах и для успешной аутентификации требуется выполнение двух условий: физическое наличие самого USB-токена и знание PIN-кода к нему?

40.Какое персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживает работу с цифровыми сертификатами и электронной цифровой подписью, исполняется в виде USB-ключей, смарт-карт, комбинированных устройств и автономных генераторов одноразовых паролей?

41.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?

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

43. 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?

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

45.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?

46.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?

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

48.Как называют технологию поиска, аккумулирования и анализа данных, собранных из доступных источников в интернете?

49. К какому виду программно-технических средств обеспечения информационной безопасности относят шифрование и цифровую подпись?

50. Что такое комплексная система защиты информации?

51. Что такое физическая защита информации?

52.Что такое техническая защита информации?

53. Что такое защита объекта?

54. Какие компоненты входят в комплекс защиты охраняемых объектов?

55.Какой подход к обеспечению информационной безопасности самый эффективный?

56. Как определить класс защищенности системы?

57.Какие существуют виды инженерно-технических средств безопасности?

58. Какие существуют возможные способы организации утечки информации?

59.Что такое технические каналы утечки информации (ТКУИ)?

60. Каким образом классифицируются каналы утечки информации?

61.Что входит в структуру канала утечки информации?

62.Каковы основные причины утечки данных?

63.Что такое защита информации от утечки?

64. Какие проблемы решает DLP-система?

65. Что называют каналом утечки речевой информации?

66. Что такое вспомогательные технические средства и системы (ВТСС)?

67.Как классифицируются акустические каналы утечки информации?

68.Какие существуют средства защиты акустической речевой информации от утечки по техническим каналам?

69.Что такое закладные устройства?

70. Какие технические средства применяют для выявления радиозакладных устройств (РЗУ)?

Составил:
Преподаватель Е.М. Грубник