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 материалы для промежуточной аттестации по МДК 03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи, МДК 03.02 Технология применения комплексной системы защиты информации в составе ПМ.03 Обеспечение информационной безопасности систем мобильной связи по специальности 11.02.08 – Средства связи с подвижными объектами

Комплексный дифференцированный зачет является промежуточной формой контроля, подводит итог освоения МДК 03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи и МДК 03.02 Технология применения комплексной системы защиты информации.

В результате освоения МДК 03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи и МДК 03.02 Технология применения комплексной системы защиты информации студент должен освоить следующие профессиональные компетенции:

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 общие компетенции:

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

Результатом освоения МДК 03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи и МДК 03.02 Технология применения комплексной системы защиты информации являются освоенные умения и усвоенные знания.

В результате освоения МДК 03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи и МДК 03.02 Технология применения комплексной системы защиты информации студент должен 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.

Вариативная часть:

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.

В результате освоения МДК 03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи и МДК 03.02 Технология применения комплексной системы защиты информации студент должен 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.

Вариативная часть.

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.

Комплексный дифференцированный зачетпо МДК03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи и МДК 03.02 Технология применения комплексной системы защиты информациипроводится в форме тестирования. Тест содержит 30вопросов (суммарно вопросы открытого и закрытого типов), выбираемых случайным образом программой из каждого блока по 15 вопросов(первый блок – задания закрытого типа – 200 тестовых вопросов в совокупности по двум МДК, второй блок – задания открытого типа – 200 теоретических вопросов с кратким ответом в совокупности по двум МДК).

Время тестирования – 90 минут (по 2 минуты на каждый вопрос тестовых позиций и по 3 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 15 минут.

Критерии оценивания:

«5 баллов» - соответствует работа, содержащая 90-100% правильных ответов;

«4 балла» - соответствует работа, содержащая 70-89% правильных ответов;

«3 балла» - соответствует работа, содержащая 50-69% правильных ответов;
«2 балла» - соответствует работа, содержащая менее 50% 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

Блок заданий закрытого типапо МДК 03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи Формируемые компетенции: ПК 3.1 – ПК 3.3, ОК 1 - ОК 9		
1.	Информационная безопасность – это…	1.Состояние защищённости информационной среды. 2.Сохранность информационных ресурсов. 3.Защита конфиденциальности, целостности и доступности информации. 4.Все ответы не верны.
2.	Какие решения направлены на обеспечение информационной безопасности?	1.Высокопроизводительные системы защиты каналов. 2.Автоматизированные системы в защищенном исполнении. 3.Защита периметра информационной системы. 4.Все ответы верны.
3.	Какие существуют уровни обеспечения защиты информации?	1.Законодательный. 2.Организационно-административный. 3.Программно-технический (аппаратный). 4.Физический. 5.Вероятностный. 6.Распределительный.
4.	Что не относится к государственным органам РФ, контролирующим деятельность в области защиты информации?	1.Комитет Государственной думы по безопасности. 2.Совет безопасности России. 3.Федеральная служба по техническому и экспортному контролю. 4.Служба экономической безопасности.
5.	Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?	1.Доступность 2.Целостность 3.Конфиденциальность 4.Управляемость 5.Надежность
6.	Что такое доступность информации?	1.Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия. 2.Свойство системы, обеспечивать беспрепятственный доступ к информации любых субъектов. 3.Свойство системы, обеспечивать закрытый доступ к информации любых субъектов. 4.Свойство информации, заключающееся в легкости ее несанкционированного получения и дальнейшего распространения (несанкционированного копирования)
7.	Что такое целостность информации?	1.Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). 2.Свойство информации, заключающееся в возможности ее изменения любым субъектом 3.Свойство информации, заключающееся в возможности

		изменения только единственным пользователем 4.Свойство информации, заключающееся в ее существовании в виде единого набора файлов.
8.	Что такое конфиденциальность информации?	1.Свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней. 2.Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). 3.Свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора. 4.Свойство информации, заключающееся в ее шифровании. 5.Свойство информации, заключающееся в ее принадлежности к определенному набору.
9.	Какие документы относятся к актам федерального законодательства?	1.Международные стандарты. 2.Международные договоры РФ. 3.Приказы ФСБ. 4.Указы президента РФ.
10.	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.
11.	Какие угрозы безопасности информации являются преднамеренными?	1.Взрыв в результате теракта. 2.Поджог. 3.Забастовка. 4.Ошибки персонала. 5.Неумышленное повреждение каналов связи. 6.Некомпетентное использование средств защиты. 7.Утрата паролей, ключей, пропусков. 8.Хищение носителей информации. 9.Незаконное получение паролей.
12.	Какие угрозы безопасности информации являются непреднамеренными?	1.Взрыв в результате теракта. 2.Поджог. 3.Забастовка. 4.Ошибки персонала. 5.Неумышленное повреждение каналов связи. 6.Некомпетентное использование средств защиты. 7.Утрата паролей, ключей, пропусков.

		8.Хищение носителей информации.
13.	Что относится к правовым мерам защиты информации?	1.Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения. 2.Действия правоохранительных органов для защиты информационных ресурсов. 3.Организационно-административные меры для защиты информационных ресурсов. 4.Действия администраторов сети защиты информационных ресурсов.
14.	Какие имеются виды правовой ответственности за нарушение законов в области информационной безопасности?	1.Уголовная 2.Административно-правовая. 3.Гражданско-правовая. 4.Дисциплинарная. 5.Материальная. 6.Условная. 7.Договорная.
15.	Что такое государственная тайна?	1.Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. 2.Сведения о состоянии окружающей среды. 3.Все сведения, которые хранятся в государственных базах данных. 4.Сведения о состоянии здоровья президента РФ. 5.Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне.
16.	Какие правовые документы решают вопросы информационной безопасности?	1.Уголовный кодекс РФ. 2.Конституция РФ. 3.Закон "Об информации, информатизации и защите информации". 4.Закон РФ "О государственной тайне". 5.Закон РФ "О коммерческой тайне". 6.Закон РФ "О лицензировании отдельных видов деятельности". 7.Закон РФ "Об образовании". 8.Закон РФ " Об электронной цифровой подписи ".
17.	Что такое коммерческая тайна?	1.Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам. 2.Информация, к которой нет доступа на законном основании. 3.Информации, обладатель которой принимает меры к охране ее конфиденциальности. 4.Информация, содержащая в учредительных документах. 5.Информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов.
18.	Какую информацию запрещено относить к информации ограниченного доступа?	1.Информацию о чрезвычайных ситуациях. 2.Информацию о деятельности органов государственной власти. 3.Документы открытых архивов и библиотек. 4.Все, перечисленное в остальных пунктах.
19.	Какой из перечисленных законодательных актов обладает наибольшей юридической силой в	1.Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне".

	вопросах информационного права?	2.ГК РФ. 3.Закон "Об информации, информатизации и защите информации". 4.Конституция РФ.
20.	Что понимается под средствами физического управления доступом?	1.Механические, электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к защищаемой информации. 2.Силовые действия охраны организации против потенциальных нарушителей. 3.Указания в инструкциях на мероприятия по подержанию физической формы сотрудников 4.Программные меры защиты, предназначенные для создания препятствий потенциальным нарушителям. 5.Информационное обеспечение секретных задач.
21.	Как называется нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий?	1.Профилем защиты. 2.Профилем безопасности. 3.Стандартом безопасности. 4.Системой защиты.
22.	Что является недостатком модели политики безопасности на основе анализа угроз системе?	1.Изначальное допущение вскрываемости системы. 2.Необходимость дополнительного обучения персонала. 3.Сложный механизм реализации. 4.Статичность.
23.	Что является наилучшим описанием количественного анализа рисков?	1.Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности. 2.Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков. 3.Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков. 4.Метод, основанный на суждениях и интуиции.
24.	Почему при проведении анализа информационных рисков следует привлекать специалистов из различных подразделений компании?	1.Чтобы убедиться, что проводится справедливая оценка. 2.Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ. 3.Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа. 4.Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку.
25.	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.
26.	Что из перечисленного является угрозами конфиденциальности информации:	1.Маскарад. 2.Карнавал. 3.Переадресовка. 4.Перехват данных. 5.Блокирование. 6.Злоупотребления полномочиями.

27.	Какая категория лиц является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?	1.Сотрудники. 2.Хакеры. 3.Атакующие. 4.Контрагенты (лица, работающие по договору).
28.	Что подразумеваетпринцип «разделение обязанностей»?	1.Для выполнения критических или необратимых операций требуется участие нескольких независимых пользователей. 2.Данный принцип требует создания механизма подотчётности пользователей, позволяющего отследить моменты нарушения целостности информации. 3.Порядок передачи привилегий должен полностью соответствовать организационной структуре предприятия.
29.	Что такое процедура?	1.Правила использования программного и аппаратного обеспечения в компании. 2.Пошаговая инструкция по выполнению задачи. 3.Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах. 4.Обязательные действия.
30.	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?	1.Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски. 2.Когда риски не могут быть приняты во внимание по политическим соображениям. 3.Когда необходимые защитные меры слишком сложны. 4.Когда стоимость контрмер превышает ценность актива и потенциальные потери.
31.	Какая из приведенных техник является самой важной при выборе конкретных защитных мер?	1.Анализ рисков. 2.Анализ затрат / выгоды. 3.Результаты ALE. 4.Выявление уязвимостей и угроз, являющихся причиной риска.
32.	Что из перечисленного не является целью проведения анализа рисков?	1.Делегирование полномочий. 2.Количественная оценка воздействия потенциальных угроз. 3.Выявление рисков. 4.Определение баланса между воздействием риска и стоимостью необходимых контрмер.
33.	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.
34.	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.

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.	Какая угроза возникает всякий раз, когда в результате преднамеренных действий умышленно блокируется доступ к некоторому ресурсу информационной системы?	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
37.	Какая угроза заключается в том, что информация становится известна неавторизованному пользователю?	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
38.	Какая угроза включает в себя любое несанкционированное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую?	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
39.	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.
40.	На сколько групп разделены классы автоматизированных систем согласно специфическим особенностям обработки информации в Руководящем документе ГТК «Классификация автоматизированных систем и требований по защите информации»?	1. 4 группы. 2. 7 групп. 3. 3 группы. 4. 2 группы. 5. 5 групп.
41.	К какой группе относятся АСОД, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности?	1.Третья группа. 2.Вторая группа. 3.Первая группа. 4.Четвертая группа.
42.	К какой группе относятся АСОД, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности?	1.Третья группа. 2.Вторая группа. 3.Первая группа. 4.Четвертая группа.
43.	К какой группе относятся	1.Третья группа.

	многопользовательскиеАСОД, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют разные права на доступ к информации?	2.Вторая группа. 3.Первая группа. 4.Четвертая группа.
44.	На сколько групп классы защищенности СВТ подразделяются в зависимости от реализованных моделей защиты и надежности их проверки?	1.Две группы. 2.Три группы. 3.Четыре группы. 4. Шесть групп.
45.	Какая группа классов защищенности СВТ включает только один седьмой класс - минимальная защищенность?	1.Первая группа. 2.Вторая группа. 3.Третья группа. 4. Четвертая группа.
46.	Какая группа классов защищенности СВТ характеризуется избирательной защитой, которая предусматривает контроль доступа поименованных субъектов к поименованным объектам, и включает шестой и пятый классы?	1.Первая группа. 2.Вторая группа. 3.Третья группа. 4. Четвертая группа.
47.	Какая группа классов защищенности СВТ характеризуется полномочной защитой, которая предусматривает присвоение каждому субъекту и объекту системы классификационных меток, указывающих место субъекта объекта в соответствующей иерархии, и включает 4, 3 и 2 классы?	1.Первая группа. 2.Вторая группа. 3.Третья группа. 4. Четвертая группа.
48.	Какая группа классов защищенности СВТ характеризуется верифицированной защитой и содержит только первый класс?	1.Первая группа. 2.Вторая группа. 3.Третья группа. 4. Четвертая группа.
49.	Сколько классов защищенности СВТ установлено в Руководящем документе ГТК?	1. 6 классов защищенности. 2. 7 классов защищенности. 3. 9 классов защищенности. 4. 5 классов защищенности. 5. 8 классов защищенности.
50.	Какие бывают виды электронной подписи?	1.Простая и усиленная 2.Усиленная и сертифицированная. 3.Простая и квалифицированная.
51.	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.
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.	Какая электронная подпись (ЭП) дополнительно подтверждается сертификатом, выданным аккредитованным удостоверяющим центром?	1.Усиленая неквалифицированная ЭП. 2. Усиленная квалифицированная ЭП. 3. Простая ЭП. 4.Сложная ЭП.
54.	Какие объекты относятся к критической информационной	1. Информационные системы. 2. Телекоммуникационные сети.

	инфраструктуре (КИИ)?	3.Автоматизированные системы управления технологическими процессами. 4. Все, перечисленное в остальных пунктах.
55.	Как называют единый территориально распределенный комплекс центров различного масштаба, обменивающихся информацией о кибератаках?	1.Критическая информационная инфраструктура (КИИ). 2.Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). 3.Межгосударственная нормативно-методическая комиссия (МНМК). 4.Система оперативно-розыскных мероприятий (СОРМ).
56.	Как называют документ, устанавливающий требования, спецификации, руководящие принципы или характеристики, 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.
57.	Какие из перечисленных функций являются основными функциями ФСТЭК?	1.Проведение единой технической политики и координация работ по защите информации 2.Организация и контроль над проведением работ по защите информации в организациях и учреждениях от утечки по техническим каналам, от НСД к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения. 3.Поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации. 4. Все, перечисленное в остальных пунктах.
58.	Что такое техническая защита 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.
59.	Что такое физическая защита 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.
60.	Что такое криптографическая защита 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.
61.	Какие угрозы называют естественными угрозами?	1.Угрозы ИБ АС, вызванные деятельностью человека. 2.Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека. 3. Угрозы, вызванные воздействиями на АС и ее компоненты физических процессов, зависящими от человека.
62.	Какие угрозы называют искусственными угрозами?	1.Угрозы ИБ АС, вызванные деятельностью человека. 2.Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека. 3. Угрозы, вызванные воздействиями на АС и ее компоненты физических процессов, независящими от человека.
63.	Что такое модель угроз информационной безопасности?	1. Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека. 2. Описание существующих угроз ИБ, их актуальности, возможности реализации и последствий. 3.Угрозы ИБ АС, вызванные деятельностью человека.
64.	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»
65.	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»
66.	Межсетевые экраны какого типа предназначены для размещения на мобильных или стационарных узлах 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»
67.	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»
68.	Межсетевые экраны какого типа работают с промышленными протоколами передачи данных?	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»
69.	Сколько классов систем обнаружения вторжений выделено регулятором?	1.Четырехуровненевая классификация систем обнаружения вторжений. 2.Шестиуровневая классификация систем обнаружения вторжений. 3.Трехуровневая классификация систем обнаружения вторжений.
70.	Какая система обнаружения	1.Система уровня приложений.

	вторжений подключается к коммуникационному оборудованию и контролирует сетевой трафик, наблюдая за несколькими сетевыми узлами?	2.Система уровня сети. 3.Система уровня узла. 4.Система уровня системных вызовов.
71.	Какая система обнаружения вторжений устанавливается на узел и проводит анализ системных вызовов, журналов работы приложений?	1.Система уровня приложений. 2.Система уровня сети. 3.Система уровня узла. 4.Система уровня системных вызовов.
72.	Сколько классов защищенности средств антивирусной защиты информации выделено регулятором?	1.Четырехуровненевая классификация средств антивирусной защиты. 2.Шестиуровневая классификация средств антивирусной защиты. 3.Трехуровневая классификация средств антивирусной защиты.
73.	Какие типы средств антивирусной защиты выделяет ФСТК России?	1.Средства антивирусной защиты, предназначенные для централизованного администрирования средств антивирусной защиты, установленных на компонентах информационных систем (тип «А»). 2.Средства антивирусной защиты, предназначенные для применения на серверах (тип «Б»). 3.Средства антивирусной защиты, предназначенные для применения на автоматизированных рабочих местах (тип «В»). 4.Средства антивирусной защиты, предназначенные для применения на автономных автоматизированных рабочих местах (тип «Г»). 5. Все, перечисленное в остальных пунктах.
74.	Сколько существует классов защиты средств доверенной загрузки?	1.Четырехуровненевая классификация средств доверенной загрузки. 2.Шестиуровневая классификация средств доверенной загрузки. 3.Трехуровневая классификация средств доверенной загрузки. 4.Пятиуровневая классификация средств доверенной загрузки.
75.	Какие типы средств доверенной загрузки выделяет ФСТК России?	1.Средства доверенной загрузки уровня базовой системы ввода-вывода. 2.Средства доверенной загрузки уровня платы расширения. 3.Средства доверенной загрузки уровня загрузочной записи. 4. Все, перечисленное в остальных пунктах.
76.	Сколько существует классов защиты средств контроля съемных машинных носителей?	1.Четырехуровненевая классификация контроля съемных машинных носителей. 2.Шестиуровневая классификация средств контроля съемных машинных носителей. 3.Трехуровневая классификация средств контроля съемных машинных носителей. 4.Пятиуровневая классификация средств контроля съемных машинных носителей.
77.	Какие различают типы средств контроля съемных машинных носителей информации?	1.Средства контроля подключения съемных носителей информации. 2.Средства контроля отчуждения (переноса) информации со съемных машинных носителей. 3.Средства контроля загрузки съемных носителей информации. 4.Средства контроля взаимодействия съемных носителей информации.

78.	Операционные системы какого типа устанавливаются на средства вычислительной техники общего назначения, такие как АРМ, серверы, смартфоны, планшеты, телефоны?	1.Операционные системы типа «А». 2.Операционные системы типа «Б». 3.Операционные системы типа «В».
79.	Операционные системы какого типа устанавливаются в специализированные технические средства, решающие заранее определенные наборы задач?	1.Операционные системы типа «А». 2.Операционные системы типа «Б». 3.Операционные системы типа «В».
80.	Операционные системы какого типа предназначены для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности?	1.Операционные системы типа «А». 2.Операционные системы типа «Б». 3.Операционные системы типа «В».
81.	Какие виды средств защиты информации должны содержатьсяв 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.
82.	Какие виды средств криптографической защиты информации определено 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.
83.	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.
84.	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.
85.	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.
86.	Какие СЗИ обеспечивают защиту от	1.Средства электронной подписи.

	навязывания ложной информации, возможность обнаружения изменений информации с помощью реализованных в СЗИ криптографических механизмов?	2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты 5.Средства шифрования.
87.	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.
88.	Сколько классов криптографических средств защиты информации определено ФСБ России?	1.Шесть классов. 2.Пять классов. 3.Семь классов. 4.Четыре класса.
89.	Как условно разделяются ценные активы организации в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»?	1. Временные и финансовые. 2.Основные и вспомогательные. 3.Неопределенные и определенные.
90.	Что из перечисленного относится к основным активам организации?	1. Место функционирования организации - пределы контролируемой зоны, в которой функционирует информационная система. 2. Бизнес-процессы - совокупность различных видов деятельности, в результате которой создается продукт или услуга, представляющие интерес для потребителя. 3. Информация - сведения, являющиеся предметом собственности, подлежащие защите от нарушения конфиденциальности, целостности и доступности, в соответствии с требованиями правовых документов и требованиями владельца информации, вне зависимости от формы представления. 4.Сведения, компрометация которых никаким образом не повлияет на деятельность организации.
91.	Что из перечисленного относится к вспомогательным активам организации?	1. Место функционирования организации - пределы контролируемой зоны, в которой функционирует информационная система. 2. Бизнес-процессы - совокупность различных видов деятельности, в результате которой создается продукт или услуга, представляющие интерес для потребителя. 3.Сведения, компрометация которых никаким образом не повлияет на деятельность организации. 4.Аппаратно-программный комплекс – совокупность технических и программных средств, предназначенных для выполнения взаимосвязанных эксплуатационных функций по обработке информации ограниченного распространения, включающая в себя активную аппаратуру обработки данных, стационарную аппаратуру, периферийные обрабатывающие устройства, операционные системы и прикладное программное обеспечение. 5.Носители данных - носитель для хранения данных, включая электронный носитель и аналоговый. 6. Сеть - совокупность телекоммуникационных устройств, используемых для соединения нескольких физически удаленных сегментов информационной системы.

		7. Персонал - все субъекты, имеющие легитимный доступ в пределах контролируемой зоны и являющиеся потенциальными внутренними нарушителями.
92.	Какой процесс понимается под идентификацией риска?	1. Процесс оценки и обработки рисков. 2.Процесс нахождения и определения рисков ИБ. 3. Коммуникация риска.
93.	Какой процесс понимается под оценкой риска?	1. Присвоение числовых значений последствиям реализации риска, а также вероятности его реализации. 2.Процесс нахождения и определения рисков ИБ. 3. Коммуникация риска.
94.	Какой документ определяет порядок выполнения отдельных или взаимосвязанных действий, выполняемых конкретным подразделением или работником организации в рамках определенных процессов ИБ?	1.Типовой сценарий. 2.Регламент. 3. Описание требований и методов работы. 4.Инструкция.
95.	Какие важные задачи решаются при создании системы физической защиты (СФЗ) объекта?	1.Установку режимов доступа, прием и обработка информации со считывателей. 2.Предотвращение несанкционированного проникновения нарушителя на объект с целью хищения или уничтожения активов организации. 3.Защита объекта от воздействия стихийных сил и прежде всего, пожара и воды.
96.	Какие мероприятия по управлению ИБ реализуют при размещении оборудования?	1.Оборудование необходимо размещать так, чтобы свести до минимума излишний доступ в места его расположения. 2.Средства обработки и хранения важной информации следует размещать так, чтобы уменьшить риск несанкционированного наблюдения за их функционированием. 3.Должны быть сведены к минимуму риски потенциальных угроз ИБ, включая: воровство; пожар; взрыв; задымление; затопление; пыль; вибрацию; химические эффекты; помехи в электроснабжении; электромагнитное излучение. 4.Важно проводить мониторинг состояния окружающей среды для выявления условий, которые могли бы неблагоприятно повлиять на функционирование СОИ. 5.Необходимо разработать меры по ликвидации последствий бедствий, случающихся в близлежащих помещениях, например, пожар в соседнем здании, затопление в подвальных помещениях или протекание воды через крышу, взрыв на улице. 6. Все, перечисленное в остальных пунктах.
97.	Каким образом обеспечивают подачу электропитания при перебоях в подаче электроэнергии и других сбоях, связанных с электричеством?	1.Наличие нескольких источников электропитания. 2.Применение устройств бесперебойного электропитания (UPS). 3.Использование резервного генератора, если необходимо обеспечить функционирование оборудования в случае длительного отказа подачи электроэнергии от общего источника. 4. Все, перечисленное в остальных пунктах.
98.	Какие мероприятия проводят для силовых и телекоммуникационных кабельных сетей, по которым передаются данные или предоставляются другие ИТ-сервисы, для защиты от перехвата информации	1.Силовые и телекоммуникационные линии, связывающие СОИ, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой. 2.Сетевой кабель должен быть защищен от несанкционированных подключений или повреждения,

	или повреждения?	например, посредством использования специального кожуха и/или выбора маршрутов прокладки кабеля в обход общедоступных участков. 3.Применение устройств бесперебойного электропитания (UPS). 4.Силовые кабели должны быть отделены от коммуникационных, чтобы исключить помехи. 5.Использование бронированных кожухов, закрытых помещений/ящиков в промежуточных пунктах контроля и конечных точках, дублирующих маршрутов прокладки кабеля или альтернативных способов передачи, оптико-волоконных линий связи, а также проверки на подключение несанкционированных устройств к кабельной сети.
99.	Для обеспечения непрерывной работоспособности и целостности в организации постоянно проводится надлежащее техническое обслуживание (ТО) оборудования. Какие меры следует применять для этих целей?	1.Оборудование следует обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком. 2.Необходимо, чтобы ТО и ремонт оборудования проводились только санкционированными лицами (персоналом). 3.Следует хранить записи обо всех случаях, предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного ТО. 4.Необходимо принимать соответствующие меры безопасности при отправке оборудования для ТО за пределы организации. 5. Все, перечисленное в остальных пунктах.
100.	Служебная информация может быть скомпрометирована вследствие небрежной утилизации (списания) или повторного использования оборудования. Какие мероприятия по управлению ИБ следует применять в этом случае?	1.Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать защищенным образом. 2.Использовать стандартные функции удаления. 3.Все компоненты оборудования, содержащего носители данных (встроенные жесткие диски), следует проверять на предмет удаления всех важных данных и лицензионного ПО. 4.Проводить оценку риской в отношении носителей данных, содержащих важную информацию, с целью определения целесообразности их разрушения, восстановления или выбраковки.

Блок заданий открытого типа по МДК 03.01 Технология применения программно-аппаратных средств защиты информации в системах мобильной связи
Формируемые компетенции: ПК 3.1 – ПК 3.3, ОК 1 - ОК 9

1.Преднамеренное указание неверных данных при заключении контракта или невыполнение абонентом контрактных условий оплаты, когда нарушитель с самого начала не планирует платить за услуги или же в какой-то момент времени отказывается от их отплаты называется?

2. Проникновение в компьютерную систему безопасности для удаления механизмов защиты или переконфигурирования системы с целью несанкционированного использования сети называется?

3. Неправомочное изготовление (клонирование) телефонных трубок или платежных телефонных карточек с фальшивыми идентификаторами абонентов, номеров и платежных отметок называется?

4.Неправомочное вмешательство в бизнес-процедуры (например, биллинг) с целью уменьшения оплаты услуг связи называется?

5. Для идентификации мошенничества важно определить его источники, от которых исходит угроза. Перечислите основные виды мошенничества?

6. Определите вид мошенничества: клонирование SIM-карт, телефонных трубок, позволяющее мошенникам совершать бесплатные вызовы в любых направлениях, так как счет за предоставленные услуги связи придет законному владельцу SIM-карты?

7. Что такое угроза информационной безопасности?

8. Что такое конфиденциальность информации?

9. Что такое целостность информации?

10. Что такое доступность информации?

11. В чем заключается угроза раскрытия информации?

12. В чем заключается угроза целостности?

13. Когда возникает угроза отказа служб?

14. Что понимают под контролируемой зоной?

15. Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или АС, преднамеренное обращение субъекта к компьютерной информации, доступ к которой ему не разрешен, независимо от цели обращения – это?

16. Какая информация относится к коммерческой тайне?

17. Что понимают под политикой безопасности?

18. В чем заключается режим разграничения доступа?

19. Какая деятельность называется защитой информации?

20. Разработка законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением, называется?

21. Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств, называется?

22. Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты – это?

23. Что обычно понимают под угрозой?

24. Как называется попытка реализации угрозы и тот, кто предпринимает такую попытку?

25.Что называют естественными угрозами?

26.Что называютискусственными угрозами?

27. Что понимают под моделью угроз информационной безопасности?

28. При построении модели угроз безопасности часто возникают сложности с выявлением и указанием факторов риска, которые могут быть реализованы в ИС. Упростить работу возможно используя банк данных угроз безопасности информации ФСТЭК России. Где находится эта электронная база?

29.Какая структура определяет порядок и координирует действия обеспечения некриптографическими методами ИБ?

30. Какая структура определяет порядок и координирует действия обеспечения криптографическими методами ИБ?

31. Как называется документ, устанавливающий требования, спецификации, руководящие принципы или характеристики, в соответствии с которыми могут использоваться материалы, продукты, процессы и услуги, которые подходят для этих целей?

32. Как называется совокупность требований в части защиты СВТ и АС?

33.Так как любое СЗИ содержит некий программный код, то можно предположить, что он обладает функциональностью, способствующей организации успешных атак в отношении защищаемых объектов. Как называются такие возможности, не указанные в документации, использование которых может привести к нарушению ИБ?

34. Сколько определено уровней контроля на отсутствие недекларированных возможностей?

35.Сколько определено ФСТЭК классов защищенности средств вычислительной техники?

36.Сколько определено ФСТЭК классов защищенности автоматизированных систем?

37.Перечислите основные уровни обеспечения защиты информации?

38.Режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, называется?

39.Защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах государственного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости, называется?

40.Обязанность не разглашать того, что стало известно лицу в силу его профессиональной деятельности (тайна исповеди, врачебная, адвокатская, нотариальная, служебная (канцелярская), тайна совещаний присяжных заседателей) называется?

41.Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации, называются?

42.В РФ устанавливаются тристепени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений, перечислите их?

43.Любые сведения о физическом лице, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, называются?

44.Что такое модель нарушителя информационной безопасности?

45.С какой целью проводится анализ защищенности?

46.Какой способ защиты информации заключается в создании на пути возникновения или распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры?

47.Какой способ защиты информациипредполагает преобразования информации, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется?

48.К каким способам защитыинформации относятся криптографические методы преобразования информации, скрытие объекта, дезинформация и легендирование, а также меры по созданию шумовых полей, маскирующих информационные сигналы?

49.К какому способу защиты информации относится разработка таких правил обращения с конфиденциальной информацией и средствами ее обработки, которые позволили бы максимально затруднить получение этой информации злоумышленником?

50.Как называется способ защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности?

51.Как называется способ защиты информации, при котором пользователи и персонал объекта внутренне (материальными, моральными, этическими, психологическими и другими мотивами) побуждаются к соблюдению всех правил обработки информации?

52.Какие средства защиты информации относятся к формальным средствам?

53.Какие средства защиты информации относятся кнеформальным средствам?

54. К каким средствам защиты относятся механические, электрические, электромеханические и т.п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов?

55.К каким средствам защиты относятсяразличные электронные и электронно-механические устройства, схемно- встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации?

56.Какие средства защиты объединены в класс технических средств защиты информации?

57.К каким средствам защиты относятсяспециальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем с целью решении задач защиты информации?

58.К каким средствам защиты относятсяспециально предусматриваемые в технологии функционирования объекта организационно-технические мероприятия для решения задач защиты информации, осуществляемые в виде целенаправленной деятельности людей?

59.К каким средствам защиты относятсясуществующие в стране или специально издаваемые нормативно-правовые акты, с помощью которых регламентируются права и обязанности, связанные с обеспечением защиты информации, всех лиц и подразделений, имеющих отношение к функционированию системы, а также устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации?

60.К каким средствам защиты относятсясложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе?

61.Какие средства защиты используются для проведения анализа защищенности?

62.Что понимается под термином «безопасность» в стандарте GSM?

63. В основе безопасности GSM лежат три алгоритма, которые являются официально закрытыми, т.е. секретными, перечислите их?

64.Что содержит реестридентификацииоборудованияEIR?

65. Какие списки формируетреестр идентификации оборудования EIR?

66.Какие списки, формируемые реестром идентификации оборудования, используются у российских операторов (и большей части операторов стран СНГ)?

67.Где производится аутентификация абонента, а точнее - SIM?

68. Как называется документ, определяющий порядок взаимодействия подразделений и работников организации в рамках определенного процесса ИБ?

69.Как называется документ, определяющий порядок выполнения отдельных или взаимосвязанных действий конкретным работником организации в рамках определенных процессов ИБ?

70.Какой документ определяет унифицированные правила и методы выполнения действий (функций), независимые от исполнителей?

71.На какие группы подразделяются категории обрабатываемых персональных данных?

72.К какой группе ПДнотносится информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информация о здоровье и интимной жизни субъект?

73.К какой группе ПДн относятся данные, характеризующие биологические или физиологические особенности субъекта, например, фотография или отпечатки пальцев?

74.К какой группе ПДн относятся сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом?

75. Сколько уровней защищенности персональных данных устанавливается в ИС при обработке персональных данных?

76.Для каких целей используется физическая защита информации?

77.Совокупность средств контроля и управления физическим доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью, называются?

78. Какие задачи решаются при создании системы физической защиты?

79. Что такое периметр безопасности?

80. Какие средства, реализующие контроль за информацией, направленной в АС или исходящей из нее, выполняющие фильтрацию информации по заданным критериям, рассматриваются ФСТЭК в качестве СЗИ?

81.Какие средства автоматизируют процесс контроля событий в сети с проведением анализа этих событий с целью поисках признаков инцидента ИБ?

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

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

84.Какие типы межсетевых экранов определены ФСТЭК России?

85. Какие типы средств антивирусной защиты Вы знаете?

86. Какие типы средств доверенной загрузки выделено ФСТЭК?

87. Какой регулятор ИБ осуществляет организацию и контроль над проведением работ по защите информации в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от НСД к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения?

88. Какой регулятор ИБ осуществляет поддержание и развитие сегмента международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации», а также за безопасность системы межведомственного электронного документооборота?

89. Как называется единый территориально распределенный комплекс центров различного масштаба, обменивающихся информацией о кибератаках?

90. Что входит в состав объектов критической информационной инфраструктуры?

91. Как называют информацию 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?

92. Что подтверждает простая ЭП?

93.Что подтверждает усиленная неквалифицированная ЭП?

94.Что подтверждает усиленная квалифицированная ЭП?

95. Является ли разработка, изготовление и распространение криптографических средств защиты информации лицензируемым видом деятельности?

96. Если криптографическое СЗИ может противостоять атакам при наличии физического доступа к средствам вычислительной техники с установленными криптографическими СЗИ, то такое СЗИ соответствует классу?

97. 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 такое СЗИ соответствует классу?

98.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 такое СЗИ соответствует классу?

99.Какие криптографические СЗИ, обеспечивают возможность разграничения доступа к информации?

100.Какие классы криптографических СЗИ определены ФСБ России?

Блок заданий закрытого типа по МДК 03.02 Технология применения комплексной системы защиты информации Формируемые компетенции: ПК 3.1 – ПК 3.3, ОК 1 – ОК 9		
1.	Что из перечисленного всегда является уязвимостью?	1.Слабое место в системе, с использованием которого может быть осуществлена атака. 2. Ошибка в программном обеспечении. 3.Отсутствие политики безопасности. 4.Ошибка в настройках межсетевого экрана.
2.	Что понимается под атакой на информационную систему	1Любое действие, нарушающее безопасность информационной системы. 2.Действие или последовательность связанных между собой действий, использующих уязвимости данной информационной системы и приводящих к нарушению политики безопасности.

		3.Использование ошибки в программном обеспечении. 4.Исключительно несанкционированный доступ в систему.
3.	Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется?	1.Мониторинг. 2.Аудит. 3.Управление ресурсами. 4.Администрирование.
4.	Из каких подсистем состоит dIDS?	1.Центральный анализирующий сервер. 2.Агенты сети. 3.Сервер сбора информации об атаке. 4.Система сбора и анализа событий, генерируемых различными типами СЗИ.
5.	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.
6.	На основании каких факторов выбираются полезные источники и правила корреляции SIEM систем?	1.Критичность системы (ценность, риски) и информации (обрабатываемой и хранимой). 2.Достоверность и информативность источника событий. 3.Покрытие каналов передачи информации. 4.Решение спектра задач ИТ и ИБ (обеспечение непрерывности, расследование инцидентов, соблюдение политик, предотвращение утечек информации и т. п.). 5.Все ответы верны.
7.	Что такое сервис безопасности?	1.Сервис, который обеспечивает задаваемую политикой безопасность информационных систем и/или передаваемых данных. 2.Сервис, который определяет осуществление атаки. 3.Сервис, который предотвращает несанкционированный доступ к файлам и программам. 4.Сервис, который обеспечивает взаимодействие с вышестоящей организацией.
8.	Что из перечисленного не относится к сервисам безопасности?	1.Используемые математические алгоритмы. 2.Предотвращение несанкционированного доступа. 3.Обнаружение и документирование проникновения. 4.Выполнение аутентификации сервера.
9.	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.
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 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.	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.
14.	Что такое авторизация?	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.
15.	В чем состоит основное назначение межсетевого экрана?	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.
16.	Что понимается под термином «сетевой периметр»?	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.
17.	Какие политики считаются для межсетевого экрана политиками по умолчанию?	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.
18.	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.

19.	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.
20.	Какие вирусы активизируются в самом начале работы с операционной системой?	1.Троянцы. 2.Загрузочные вирусы. 3.Черви.
21.	Межсетевого экрана какого класса не существует?	1.Экранирующий маршрутизатор. 2.Экранирующий коммутатор. 3.Экранирующий транспорт. 4.Экранирующий шлюз.
22.	Какую аутентификацию рекомендуется использовать при удаленном доступе?	1.Однофакторную. 2.Двухфакторную. 3.Трехфакторную.
23.	Какие записи должны вестись при аудите?	1.Вход/выход пользователей. 2.Неудачные попытки входа. 3.Все системные события 4.Зависит от уровня аудита.
24.	Каковы преимущества частных сетей?	1.Информация 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.
25.	Как называется приложение, которое хочет предоставлять сервис, доступный по сети другим приложениям?	1.Клиентом. 2.Коммутатором. 3.Маршрутизатором. 4.Сервером.
26.	Как можно охарактеризовать 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.
27.	Каким образом определяется тип межсетевого экрана?	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.
28.	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.
29.	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.
30.	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.
31.	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.
32.	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.
33.	Какие преимущества имеет централизованное управление идентификационными и аутентификационными данными?	1.Возможность использования многофакторной аутентификации. 2.Возможность использования цифровых подписей. 3.Легкое администрирование. 4.Возможность использования третьей доверенной стороны.
34.	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.
35.	Что из перечисленного является основными компонентами управления доступом?	1.Субъекты. 2.Маршрутизаторы. 3.Объекты или ресурсы. 4.Разрешения (привилегии).
36.	Какие функции НЕ выполняет антивирусная защита?	1.Поиск и уничтожение известных вирусов. 2.Поиск и уничтожение неизвестных вирусов. 3.Определения адреса отправителя вирусов.
37.	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.
38.	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).
39.	Что относится к идентификации и/или аутентификации людей на основе их физиологических характеристик?	1.Анализ особенностей голоса. 2.Распознавание речи; 3.Отпечатки пальцев; 4.Сканирование радужной оболочки глаза; 5.Анализ знаний по информационной безопасности. 6.Анализ динамики подписи (ручной).
40.	Что относится к идентификации и/или аутентификации людей на основе их поведенческих характеристик?	1.Анализ динамики подписи (ручной). 2.Анализ стиля работы с клавиатурой. 3.Анализ отпечатков пальцев. 4.Анализ административных указаний по информационной безопасности. 5.Анализ тембра голоса.
41.	Что из перечисленного является наиболее точными способами идентификации человека?	1.Удостоверение личности с фотографией (паспорт). 2.Отпечатки пальцев (папиллярные узоры). 3.Узор радужной оболочки или сетчатки глаза.
42.	Что из перечисленного является сервером VPN?	1.Любой компьютер в сети 2.Компьютер в сети, выступающий в роли конечного узла. 3.Компьютер к которому могут подключаться пользователи.
43.	Что из перечисленного относится к аппаратным средствам аутентификации?	1.Электронные ключи. 2.Смарт-карты. 3.S/KEY. 4.Kerberos.
44.	Выберите из предложенных вариантов пароля "правильный" (с точки зрения современных требований к паролю)?	1.1rR%56ty. 2.i23Y65. 3.mersqwertyp. 4.3488714567747865.
45.	Некоторая уникальная информация, позволяющая различать пользователей называется?	1.Идентификатор (логин). 2.Пароль. 3.Учетная запись. 4.Ключ.
46.	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.
47.	Совокупность идентификатора и пароля пользователя называется?	1.Логин пользователя. 2.Учетная запись пользователя. 3.Ключ пользователя.
48.	Как называется присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных?	1.Идентификацией пользователя. 2.Аутентификацией пользователя. 3.Опознанием пользователя. 4.Созданием учетной записи пользователя.
49.	Как называется проверка принадлежности пользователю предъявленного им идентификатора?	1.Идентификацией пользователя. 2.Аутентификацией пользователя. 3.Регистрацией пользователя. 4.Созданием учетной записи пользователя.
50.	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.
51.	Что понимается под DoS-атакой?	1.Модификация передаваемого сообщения. 2.Повторное использование нарушителем перехваченного ранее сообщения. 3.Невозможность доступа в систему законным пользователем. 4.Невозможность получения сервиса законным пользователем.
52.	Невозможность получения сервиса законным пользователем называется?	1.DoS-атакой. 2.Replay-атакой. 3.Пассивной атакой. 4.Атакой «man-in-the-middle».
53.	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.
54.	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.
55.	Где лучше размещать VPN сервер?	1.В отдельной DMZ. 2.В DMZ интернета, вместе с остальными серверами. 3.Во внутренней сети компании.
56.	Какой должна быть система аутентификации, использующаяся в VPN?	1.Однофакторной. 2.Двухфакторной. 3.Трехфакторной. 4.Четырехфакторной.
57.	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.
58.	Какое средство аутентификации рекомендуется использовать в VPN?	1.Смарт-карту и пароль. 2.Только смарт-карту. 3.Только пароль. 4.Биометрическую идентификацию.
59.	В чем состоит атака IP Spoofing?	1.Нарушитель изменяет IP-адрес получателя на IP-адрес доверенного хоста. 2.Нарушитель изменяет содержимое протокола прикладного уровня. 3. Нарушитель изменяет IP-адрес источника на IP-адрес доверенного хоста. 4.Нарушитель изменяет номер порта получателя.
60.	Какие из указанных контрмер позволяют компенсировать физические уязвимости?	1.Межсетевые экраны. 2.Устройства считывания смарт-карт при входе в помещения. 3.Охрана.

		4.Шифрование.
61.	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.
62.	Наличие какого элемента характерно для всех архитектур DMZ?	1.Почтовый сервер. 2.DNS. 3.NTP. 4.Межсетевой экран.
63.	Как расшифровывается аббревиатура DMZ?	1.Демилитаризованная зона. 2.Зона управления данными. 3.Зона ежедневного управления. 4.Зона поддержки данных.
64.	то 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.
65.	Если в организации есть веб-сервер для внешних пользователей и веб-сервер для получения информации своими сотрудниками, то оптимальным количеством DMZ является?	1.Одна DMZ. 2.Две DMZ. 3.Три DMZ. 4.Четыре DMZ.
66.	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.
67.	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.
68.	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.
69.	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.
70.	Как называется сетевая атака, целью	1.«Отказотобслуживания» (Denial of Service - DoS).

	которой является поиск открытых портов работающих в сети устройств, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих устройствах?	2.Срыв стека. 3.Внедрение на компьютер деструктивных программ. 4.Перехват передаваемой по сети информации (Sniffing). 5.Спуфинг. 6.Сканирование портов.
71.	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.
72.	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.
73.	Что следует учитывать при выборе IDS?	1.Ценность защищаемых информационных ресурсов. 2.Количество пользовательских аккаунтов в локальной сети. 3.Количество административных аккаунтов в локальной сети. 4.Загруженность сети.
74.	Какие возможности может обеспечивать IDS?	1.Возможность определения внешних угроз. 2.Возможность шифрования трафика. 3.Возможность иметь реакцию на атаку. 4.Возможность фильтрации трафика.
75.	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.
76.	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.
77.	Для чего используются системы анализа уязвимостей?	1.Для создания «моментального снимка» состояния безопасности системы. 2.Как альтернатива IDS, полностью заменяя ее. 3.Как альтернатива политики безопасности предприятия, являясь полным ее аналогом. 4.Как альтернатива межсетевым экранам, полностью заменяя их.
78.	На основании чего осуществляется управление доступом в пакетном	1.IP-адреса источника. 2.IP-адреса назначения.

	фильтре?	3.Номера привила в наборе правил пакетного фильтра. 4.Учетной записи и пароля пользователя.
79.	Что позволяет 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.
80.	Для каких целей устанавливается IDS?	1.Обнаружение атак 2.Предотвращение атак 3.Обнаружение нарушений политики 4.Повышение надежности системы.
81.	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.
82.	Какие устройства могут выполнять функции NAT?	1.Маршрутизаторы. 2.Межсетевые экраны. 3.Почтовые сервера. 4.DNS сервера.
83.	При управлении доступом на сетевом уровне для разграничения трафика используются?	1.Маршрутизаторы. 2.Межсетевые экраны. 3.Коммутаторы. 4.Веб-сервера.
84.	Какие типы аппаратных устройств могут поддерживать технологию VLAN?	1.Концентраторы. 2.Коммутаторы. 3.Межсетевые экраны. 4.Веб-серверы.
85.	Виртуальной локальной сетью (vlan) называется?	1.Логическая группа хостов в сети, трафик которой, в том числе и широковещательный, полностью изолирован на канальном уровне от хостов из других виртуальных локальных сетей. 2.Логическая группа хостов в сети, трафик которой полностью изолирован на сетевом уровне от хостов из других виртуальных локальных сетей. 3.Логическая группа хостов в сети, трафик которой полностью изолирован на прикладном уровне от хостов из других виртуальных локальных сетей. 4.Логическая группа хостов в сети, трафик которой аутентифицируется межсетевым экраном.
86.	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.
87.	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.
88.	Что необходимо обеспечить при	1.Регулярное изменение правил фильтрации.

	управлении конфигурациями?	2.Регулярное обновление ПО. 3.Управление изменениями. 4.Оценка состояния сетевой безопасности.
89.	Что из перечисленного относится к механизмам безопасности?	1.Хэш-функции. 2.Целостность сообщения. 3.Алгоритмы симметричного шифрования. 4.Аутентификация сообщения.
90.	Что из перечисленного не относится к механизмам безопасности?	1.Хэш-функции. 2.Целостность сообщения. 3.Алгоритмы симметричного шифрования. 4.Аутентификация сообщения.
91.	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.
92.	Под унифицированным управлением угрозами (UnifiedThreatManagement – 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.
93.	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.
94.	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.
95.	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.
96.	Для каких систем пригодна статическая NAT?	1.Для любых систем. 2.Для систем в DMZ. 3.Для клиентских рабочих станций.
97.	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.

98.	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.
99.	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.
100.	Как должно *всегда* выполняться администрирование межсетевого экрана?	1.По защищенному каналу. 2.Из Интернет – по защищенному каналу и с использованием строгой аутентификации. 3.Из локальной сети возможно администрирование без выполнения строгой аутентификации. 4.С использованием строгой аутентификации.

Блок заданий открытого типа
по МДК 03.02 Технология применения комплексной системы защиты информации
Формируемые компетенции: ПК 3.1 – ПК 3.3, ОК 1 – ОК 9

1.Процедура распознавания субъекта в процессе регистрации в системе называется?

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

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

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

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

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

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

8.Идентификация человека по уникальным биологическим признакам называется?

9.На какие две группы делятся методы биометрической идентификации?

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

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

12.Какой метод биометрической идентификации построен на геометрии кисти руки, когда с помощью специального устройства, состоящего из камеры и нескольких подсвечивающих диодов (включаясь по очереди, они дают разные проекции ладони), строится трехмерный образ

кисти руки, по которому формируется свертка и распознается человек?

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

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

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

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

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

18.Какие методы биометрической идентификации используются только для специализированных экспертиз, так как работают достаточно долго?

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

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

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

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

23.При каком способе аутентификации используются аутентификационные факторы нескольких типов?

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

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

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

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

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

29.При каком методе аутентификации программное или аппаратное обеспечение пользователя генерирует исходные данные, которые будут зашифрованы и отправлены на сервер

для сравнения (в процессе создания строки используется значение предыдущего запроса), сервер тоже обладает этими сведениями; зная имя пользователя, он находит значение предыдущего его запроса и генерирует по тому же алгоритму точно такую же строку, зашифровав ее с помощью секретного ключа пользователя (он также хранится на сервере), сервер получает значение, которое должно полностью совпадать с присланными пользователем данными?

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

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

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

33. Какое программное решение, выступает в роли посредника между пользователем браузера и веб-сервером, и работает по принципу ManintheMiddle, подменяя сертификаты пользователя и сервера?

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

35.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?

36.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. Как называют эту модель доступа?

37.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?

38.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?

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

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

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

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

43.Набор распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей, - это?

44.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?

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

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

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

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

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

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

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

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

53.Комплекс, предназначенный для централизованного сбора и анализа информации о событиях, поступающих из различных источников автоматизированной системы компании, называют?

54.Какая система позволяет осуществлять сравнение уязвимостей программного обеспечения с точки зрения их опасности?

55.Как называют сотрудников, которым доступна конфиденциальная информация организации, где они работают и которые могут использовать корпоративные секреты в корыстных целях, провоцируя умышленные утечки информации?

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

57.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?

58.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?

59.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?

60.Один из самых распространенных видов нежелательного программного обеспечения, предназначенный для несанкционированного сбора данных с пользовательского устройства, использующийся, например, для сбора информации о местоположении устройства, посещаемых сайтах, конфигурации компьютера, используемом программном обеспечении, вводимых с клавиатуры данных, называется?

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

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

63.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?

64.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?

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

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

67. 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?

68.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?

69.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, называют?

70.Совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов организации от угроз безопасности, называется?

71.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?

72.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?

73.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?

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

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

76.Метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника, называют?

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

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

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

80. Какую функцию выполняет межсетевой экран?

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

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

83. Каким образом работает с трафиком фильтр пакетов?

84. 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?

85. Какие виртуальные сети реализуются для обеспечения защищенного канала между корпоративной сетью и пользователем, подключенным к защищенной сети извне, например, с домашнего ПК?

86.Какие VPN реализуются провайдерами для предоставления доступа клиентам, подключающимся по одному физическому каналу?

87.Какая VPN объединяет в защищенную сеть ряд филиалов одной компании, распределенных географически, для обмена информацией по открытым каналам?

88. 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?

89. 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?

90.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?

91. 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)?

92. Какие программные и/или аппаратные средства, позволяют предотвратить попытки несанкционированного доступа, такие как неавторизованный физический доступ, доступ к файлам, хранящимся на компьютере, уничтожение конфиденциальных данных?

93.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?

94. 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?

95. Какие средства безопасности предназначены для анализа защищенности информации в корпоративных сетях и могут выполнять функции проверки сетевых устройств; проверки возможности осуществления атак типа "DenialofService", "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?

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

97. 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)?

98. 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?

99. 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?

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

Составил:
Преподаватель Грубник Е.М.