


СОГЛАСОВАНО
Начальник отдела защиты информации
Департамента цифрового развития
Смоленской области

 А.Н. Калугин
« 08. 02. 21 » г.

УТВЕРЖДАЮ
Зам. директора по УР
Иванешко И.В.
« 31 » 08 20 21 г.

Комплект оценочных материалов для промежуточной аттестации
(дифференцированный зачет – 8 семестр)
по МДК.03.01 Применение программно-аппаратных средств защиты информации
в инфокоммуникационных системах и сетях связи
ПМ.03 Обеспечение информационной безопасности инфокоммуникационных
сетей и систем связи
по специальности 11.02.15. Инфокоммуникационные сети и системы связи

Дифференцированный зачет является промежуточной формой контроля, подводит итог освоения МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи. Результатом освоения программы МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи является овладение студентами профессиональных (ПК) и общих (ОК) компетенций:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи.
ПК 3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
ПК 3.3	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.

Результатом освоения программы МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи являются освоенные умения и усвоенные знания.

В результате освоения МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи студент должен **уметь**:

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

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

- У3 - определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;
- У4 - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;
- У5 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;
- У6 - выполнять тестирование систем с целью определения уровня защищенности;
- У7 - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;
- У8 - разрабатывать политику безопасности сетевых элементов и логических сетей;
- У9 - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
- У10 - производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;
- У11 - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
- У12 - защищать базы данных при помощи специализированных программных продуктов;
- У13 - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами;
- У14 - проводить мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры;
- У15 - администрировать наложенные программно-аппаратных средства защиты информации от НСД;
- У16 - применять программно-аппаратные комплексы глубокого анализа трафика;
- У17 - вырабатывать рекомендации для принятия решения о модернизации системы защиты информации;
- У18 - осуществлять мероприятия по защите персональных данных;
- знать:
- 31 - принципы построения информационно-коммуникационных сетей;
- 32 - международные стандарты информационной безопасности для проводных и беспроводных сетей;
- 33 - нормативно - правовые и законодательные акты в области информационной безопасности;
- 34 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления и закрытия;
- 35 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
- 36 - способы и методы обнаружения средств съёма информации в радиоканале;
- 37 - классификацию угроз сетевой безопасности;
- 38 - характерные особенности сетевых атак;
- 39 - возможные способы несанкционированного доступа к системам связи;
- 310 - методы и способы защиты информации, передаваемой по кабельным направляющим системам;
- 311 - конфигурации защищаемых сетей;
- 312 - алгоритмы работы тестовых программ;
- 313 - средства защиты различных операционных систем и среды передачи информации;
- 314 - способы и методы шифрования (кодирование и декодирование) информации;
- 315 - состав работ по комплексной защите информации значимых объектов критической информационной инфраструктуры;
- 316 - методы инженерного расчета размеров контролируемой зоны;
- 317 - основные принципы организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСТЭК, ФСБ России;

318 - этапы проведения аудита информационной безопасности информационных систем и объектов информатизации.

Дифференцированный зачёт являются промежуточными формами контроля, подводят итог освоения программы МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи.

Дифференцированный зачёт по МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи проводится в форме тестирования. На промежуточную аттестацию выделяется по 2 часа (последнее занятие в семестре) из общего количества часов на МДК.03.01.

Тест содержит 30 вопросов (суммарно 20 тестовых позиций и 10 теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока заданий (первый блок – задания закрытого типа – 75 тестовых вопросов, второй блок – задания открытого типа – 75 теоретических вопросов с кратким ответом).

Время тестирования – 90 минут (по 1,5 минуты на каждый вопрос тестовых позиций и по 2 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 40 минут.

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

Критерии оценивания:

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

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

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

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

Шкала оценивания образовательных результатов:

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

Тестовое задание закрытого типа для дифференцированного зачета по МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи

1.	Какие службы из перечисленных организуют защиту информации на уровне предприятия?	1.Служба экономической безопасности. 2.Служба безопасности персонала (режимный отдел). 3.Кадровая служба. 4.Служба юридической безопасности.
2.	На какие категории разделяются кризисные ситуации, не предотвращенные СЗИ, по степени серьезности и размерам наносимого ущерба?	1.Угрожающая. 2.Умышленная. 3.Серьезная. 4.Случайная.
3.	Какими мерами из перечисленных достигается непрерывность процесса функционирования АС и своевременность восстановления ее работоспособности?	1. Постоянным поддержанием необходимого уровня защищенности компонентов системы, непрерывным управлением и административной поддержкой корректного применения средств защиты. 2.Проведением специальных регламентных мероприятий и оперативной заменой оборудования. 3.Применением различных способов резервирования аппаратных ресурсов, эталонного копирования программных и страхового копирования информационных ресурсов системы.

4.	Что из перечисленного относится к угрожающим кризисным ситуациям, не предотвращенным средствами защиты информации?	<ol style="list-style-type: none"> 1.Выход из строя рабочей станции (с потерей информации). 2.Нарушение подачи электроэнергии в здании. 3.Выход из строя файлового сервера (с потерей информации). 4.Выход из строя файлового сервера (без потери информации).
5.	Что из перечисленного относится к угрожающим кризисным ситуациям, не предотвращенные средствами защиты информации?	<ol style="list-style-type: none"> 1.Частичная потеря информации на сервере без потери его работоспособности. 2.Частичная потеря информации на рабочей станции без потери ее работоспособности. 3.Выход из строя рабочей станции (без потери информации). 4.Выход из строя локальной сети (физической среды передачи данных).
6.	Что из перечисленного относится к серьезным кризисным ситуациям, не предотвращенным средствами защиты информации?	<ol style="list-style-type: none"> 1.Выход из строя рабочей станции (с потерей информации). 2.Выход из строя рабочей станции (без потери информации). 3. Частичная потеря информации на сервере без потери его работоспособности. 4.Частичная потеря информации на рабочей станции без потери ее работоспособности.
7.	Что из перечисленного относится к ситуациям, не предотвращенным средствами защиты информации, требующим внимания?	<ol style="list-style-type: none"> 1. Частичная потеря информации на сервере без потери его работоспособности. 2.Частичная потеря информации на рабочей станции без потери ее работоспособности. 3.Несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.
8.	Какие объекты информатизации подлежат обязательной аттестации по требованиям безопасности информации?	<ol style="list-style-type: none"> 1. Объекты, предназначенные для обработки конфиденциальной информации 2.Объекты, предназначенные для обработки информации, составляющей государственную тайну. 3. Объекты, предназначенные для управления экологически опасными объектами. 4. Объекты, предназначенные для ведения секретных переговоров.
9.	Что из перечисленного обеспечивает механизм полномочного управления доступом?	<ol style="list-style-type: none"> 1.Разграничение доступа пользователей к информации, которой назначена категория конфиденциальности. 2. Обнаружение и регистрация попыток несанкционированного доступа. 3.Контроль потоков конфиденциальной информации в системе. 4.Контроль работоспособности используемых систем защиты информации.
10.	Что из перечисленного обеспечивает механизм полномочного управления доступом?	<ol style="list-style-type: none"> 1.Контроль подключения и использования устройств с назначенными категориями конфиденциальности. 2.Контроль допуска к информации для пользователей разных уровней. 3. Контроль использования сетевых интерфейсов, для которых указаны допустимые уровни конфиденциальности сессий пользователей. 4. Контроль печати конфиденциальных документов.
11.	Для каких видов устройств поддерживается теневое копирование?	<ol style="list-style-type: none"> 1.Подключаемые сменные диски. 2.Дисководы оптических дисков с функцией записи. 3.Принтеры. 4.Все ответы верны.

12.	Какие функции выполняет средство защиты информации от НСД?	<ol style="list-style-type: none"> 1.Идентификация и аутентификация пользователей и устройств. 2.Регистрация запуска (завершения) программ и процессов. 3.Управление информационными потоками между устройствами. 4.Контроль работоспособности используемых систем защиты информации.
13	Как называют сервис, который гарантирует, что информация получена из законного источника и получателем является тот, кто нужно?	<ol style="list-style-type: none"> 1.Аутентификация. 2.Авторизация. 3.Идентификация.
14.	Какую возможность вычислительной системе дает идентификация пользователя?	<ol style="list-style-type: none"> 1.Отличать одного пользователя от другого. 2.Гарантировать, что пользователь является тем, за кого он себя выдает. 3.Обеспечить корректное управление доступом. 4.Гарантировать отсутствие несанкционированного доступа.
15.	В чем заключается суть процедуры управления доступом или авторизации?	<ol style="list-style-type: none"> 1.Гарантирование того, что пользователь является тем, за кого он себя выдает. 2.Гарантирование того, что пользователь обращается к требуемому ресурсу (серверу). 3.Определение прав и разрешений пользователей по доступу к ресурсам. 4.Невозможность несанкционированного просмотра и изменения данных.
16.	Какую аутентификацию рекомендуется использовать при удаленном доступе?	<ol style="list-style-type: none"> 1.Однофакторную. 2.Двухфакторную. 3.Трехфакторную.
17.	Какие записи должны вестись при аудите информационной безопасности?	<ol style="list-style-type: none"> 1.Вход/выход пользователей. 2.Неудачные попытки входа. 3.Все системные события 4.Записи зависят от уровня аудита.
18.	В чем заключается суть многофакторной аутентификации?	<ol style="list-style-type: none"> 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.
19	Для чего нужна система контроля доступа?	<ol style="list-style-type: none"> 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 оборудование, от повреждений и кражи. 4.Все ответы верны.
20.	Как называется уникальная информация, позволяющая различать пользователей друг от друга?	<ol style="list-style-type: none"> 1.Идентификатор (логин). 2.Пароль. 3.Учетная запись. 4.Ключ.
21.	Как называют совокупность идентификатора и пароля пользователя?	<ol style="list-style-type: none"> 1.Логин пользователя. 2.Учетная запись пользователя. 3.Ключ пользователя.
22.	Какое средство аутентификации рекомендуется использовать в VPN?	<ol style="list-style-type: none"> 1.Смарт-карту и пароль. 2.Только смарт-карту.

		3.Только пароль. 4.Биометрическую идентификацию.
23.	Как называют процедуру проверки принадлежности пользователю предъявленного им идентификатора?	1.Идентификацией пользователя. 2.Аутентификацией пользователя. 3.Регистрацией пользователя. 4.Созданием учетной записи пользователя.
24.	Какие из перечисленных мер используют для повышения общего уровня защищенности сетевого периметра?	1.Постоянный контроль сетевого периметра компании с целью обнаружения сервисов, расположенных на периметре и доступных из сети Интернет. 2.Автоматизированный поиск уязвимостей в сервисах, расположенных на периметре. 3.Использование фрагментарного подхода к ИБ сервисов, расположенных на периметре.
25.	Какие из перечисленных мер используют для повышения общего уровня защищенности сетевого периметра?	1.Устранение лишних сервисов, размещение которых на периметре не обусловлено необходимостью. 2.Автоматизированный поиск уязвимостей в сервисах, расположенных на серверах компании. 3.Внедрение политики патч-менеджмента, уделение внимания системам с уязвимостями, для которых существуют эксплойты в открытом доступе, а также наиболее уязвимым системам.
26.	Решение каких задач обеспечивает система защиты информации от угроз несанкционированного доступа?	1. Задержка нарушителей, их выявление на объекте. 2.Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 3.Обеспечение функций регистрации и учета событий безопасности. 4.Обеспечение целостности программно-аппаратной среды применяемых программных и программно-технических средств. 5. Реагирование сотрудников службы безопасности.
27.	Что из перечисленного входит в состав системы защиты от несанкционированного доступа?	1.Средства централизованного управления средствами защиты от несанкционированного доступа. 2.Сертифицированные средства защиты от несанкционированного доступа. 3. Средства предупреждения несанкционированного доступа, нерегламентированных воздействий. 4.Средства удаленного администрирования АРМ и серверов, входящих в состав информационной системы.
28.	Что из перечисленного входит в состав системы защиты от несанкционированного доступа?	1.Встроенные в системное программное обеспечение средства идентификации, аутентификации, авторизации, мониторинга событий и контроля целостности. 2. Средства предупреждения несанкционированного доступа, нерегламентированных воздействий. 3.Средства резервного копирования и восстановления конфигураций средств защиты от несанкционированного доступа. 4.Средства реагирования сотрудников службы безопасности.
29.	Какие методы защиты информации могут быть использованы для предотвращения несанкционированного доступа?	1.Пароли для авторизации во время работы. 2.Регулярное создание бэкапов наиболее важных и ценных информационных массивов. 3.Криптографические средства шифрования информации для ее передачи и хранения. 4.Все ответы верны.
30.	Какие методы защиты информации могут быть использованы для предотвращения	1.Модули доверенной загрузки. 2.Средства предотвращения сетевых атак (межсетевой экран, антивирус, прокси-сервер).

	несанкционированного доступа?	3.Выполнение резервирования, дублирования компонентов информационной системы, которые связаны с хранением информации. 4.Все ответы верны.
31.	Какие существуют методы контроля аппаратной конфигурации компьютера?	1.Статический контроль конфигурации. 2.Стандартный контроль конфигурации. 3.Динамический контроль конфигурации. 4.Индивидуальный контроль конфигурации.
32.	Каковы преимущества пользовательских VPN?	1.Сотрудники, находящиеся в командировке могут подключаться к сети компании. 2.Удаленные сайты могут осуществлять обмен информацией незамедлительно. 3.Сотрудники могут работать из дома, необязательно присутствие на работе. 4.Преимуществ нет.
33.	Какие политики безопасности из перечисленных являются для межсетевое 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.
34.	Когда рекомендуется проводить работы по анализу защищенности ИТ-инфраструктуры?	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.
35.	Сколько классов защищенности АС от несанкционированного доступа к информации выделено в Руководящем документе ГТК «Классификация автоматизированных систем и требований по защите информации»?	1. 6 классов защищенности. 2. 7 классов защищенности. 3. 9 классов защищенности. 4. 5 классов защищенности. 5. 8 классов защищенности.
36.	Какие шаги следует предпринимать при обнаружении подозрительного трафика в сети?	1.Записывать в журнал сведения о дополнительном трафике между источником и пунктом назначения. 2.Заблокировать удаленную систему. 3.Записывать в журнал весь трафик, исходящий из источника. 4.Записывать в журнал содержимое пакетов из источника.
37.	Где лучше размещать VPN сервер?	1.В отдельной DMZ. 2.В DMZ интернета, вместе с остальными серверами. 3.Во внутренней сети компании.
38.	Какой должна быть система аутентификации, используемая в VPN?	1.Однофакторной. 2.Двухфакторной. 3.Трехфакторной. 4.Четырехфакторной.
39.	Что из перечисленного могут определять атаки сканирования сети?	1.Топологию целевой сети. 2.Типы сетевого трафика, пропускаемые межсетевым экраном. 3. Оценку общего состояния безопасности системы 4.Операционные системы, которые выполняются на хостах.
40.	Что из перечисленного могут определять атаки сканирования сети?	1.Программное обеспечение сервера, которое выполняется на хостах.

		<p>2.Номера версий для всего обнаруженного программного обеспечения.</p> <p>3.Аутентификационные данные пользователей.</p> <p>6.Все ответы верны.</p>
41.	Наличие какого элемента характерно для всех архитектур DMZ?	<p>1.Почтовый сервер.</p> <p>2.DNS.</p> <p>3.NTP.</p> <p>4.Межсетевой экран.</p>
42.	Каковы преимущества виртуальных частных сетей?	<p>1.Информация сохраняется в секрете.</p> <p>2.Удаленные сайты могут осуществлять обмен информацией незамедлительно.</p> <p>3.Удаленные пользователи не ощущают себя изолированными от системы, к которой они осуществляют доступ.</p> <p>4.Низкая стоимость.</p>
43.	Что такое пользовательские VPN?	<p>1.Построены между отдельной пользовательской системой и узлом или сетью организации.</p> <p>2.Используются частными пользователями для связи друг с другом.</p> <p>3.Одно из названий VPN.</p>
44.	Каким образом осуществляется доступ к внутренней сети пользователем, подключенным через VPN?	<p>1.Нужно просто знать адрес сервера VPN.</p> <p>2.Необходимо пройти процедуру аутентификации на сервере.</p> <p>3.Доступ к внутренней сети не может быть получен ни каким образом.</p>
45.	Каковы преимущества использования системы унифицированного управления угрозами?	<p>1.Увеличивается пропускная способность сети.</p> <p>2.Уменьшается сложность управления.</p> <p>3.Увеличивается безопасность сетевого периметра.</p> <p>4.Уменьшается количество попыток несанкционированного доступа.</p>
46.	Что должно располагаться в сети демилитаризованной зоны (DMZ)?	<p>1.Рабочие станции пользователей.</p> <p>2.Серверы, которые должны быть доступны только внутренним пользователям.</p> <p>3.Серверы, которые должны быть доступны из внешних сетей.</p> <p>4.Серверы, содержащие наиболее чувствительные данные.</p>
47.	Какие из перечисленных веб-серверов следует расположить во внешней DMZ?	<p>1.Веб-сервер, на котором осуществляется on-line'овый заказ услуг.</p> <p>2.Веб-сервер, на котором публикуются распоряжения руководства организации.</p> <p>3.Веб-сервер, на котором могут находиться личные данные сотрудников.</p> <p>4.Веб-сервер, на котором опубликованы общедоступные телефоны и координаты организации.</p>
48.	Как называется атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения путем создания огромного количества фальшивых запросов на доступ к ресурсам системы?	<p>1. Отказ от обслуживания</p> <p>2.Срыв стека.</p> <p>3.Внедрение на компьютер деструктивных программ.</p> <p>4.Сниффинг (Sniffing).</p> <p>5.Спуфинг.</p> <p>6.Сканирование портов.</p>
49.	Как называется атака, целью которой является трафик локальной сети?	<p>1. Отказ от обслуживания.</p> <p>2.Срыв стека.</p> <p>3.Внедрение на компьютер деструктивных программ.</p> <p>4.Сниффинг (Sniffing).</p> <p>5.Спуфинг.</p> <p>6.Сканирование портов.</p>

50.	Как называется атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой?	<ol style="list-style-type: none"> 1.«Отказ от обслуживания» (Denial of Service - DoS). 2.Срыв стека. 3.Внедрение на компьютер деструктивных программ. 4.Сниффинг (Sniffing). 5.Спуфинг. 6.Сканирование портов.
51.	Каковы преимущества использования IDS?	<ol style="list-style-type: none"> 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.
52.	Что анализируется при определении злоупотреблений?	<ol style="list-style-type: none"> 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.
53.	Что анализируется при определении аномалий?	<ol style="list-style-type: none"> 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.
54.	Какие устройства могут выполнять функции NAT?	<ol style="list-style-type: none"> 1.Маршрутизаторы. 2.Межсетевые экраны. 3.Почтовые сервера. 4.DNS сервера.
55.	Что из перечисленного понимают под унифицированным управлением угрозами (UTM)?	<ol style="list-style-type: none"> 1.Создание базы данных потенциальных угроз. 2.Создание базы данных точек входа в сеть. 3.Централизованное управление несколькими сетевыми устройствами. 4.Централизованное управление всеми межсетевыми экранами.
56.	Что включает в себя типовая система унифицированного управления угрозами?	<ol style="list-style-type: none"> 1.Межсетевой экран с возможностями определения и удаления вредоносного ПО на находящихся под его управлением хостах. 2.Рабочие станции специалистов по информационной безопасности. 3.Межсетевой экран с возможностями блокирования нежелательного трафика. 4.Сервера, предоставляющие сервисы удаленным пользователям.
57.	Какие функции из перечисленных выполняют DLP-системы?	<ol style="list-style-type: none"> 1.Контроль каналов коммуникаций, мест хранения информации, действий пользователей на рабочих станциях. 2.Управление доступом к данным и ресурсам. 3.Анализ поведения пользователей. 4.Анализ событий информационной безопасности. 5.Проведение расследований.
58.	Межсетевые экраны какого типа устанавливают на физическом периметре информационных систем?	<ol style="list-style-type: none"> 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»

59.	Где устанавливают межсетевые экраны для веб-приложений?	<p>1. После защищаемого веб-сервера (трафик вначале передается веб-серверу, затем межсетевому экрану).</p> <p>2. Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, трафик между ними запрещен.</p> <p>3. Перед защищаемым веб-сервером (трафик вначале передается межсетевому экрану, затем веб-серверу).</p> <p>4. Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, но трафик между ними не запрещен.</p>
60.	Почему существует необходимость в межсетевых экранах для виртуальных инфраструктур?	<p>1. Сетевой трафик, который передается между гостевыми ОС внутри хоста, передается в зашифрованном виде.</p> <p>2. Сетевой трафик, который передается между гостевыми ОС внутри хоста, использует протоколы, отличные от TCP/IP.</p> <p>3. Сетевой трафик, который передается между гостевыми ОС внутри хоста, не может просматриваться внешним межсетевым экраном.</p> <p>4. В сетевом трафике, который передается между гостевыми ОС внутри хоста, указаны другие номера портов, чем в обычном сетевом трафике.</p>
61.	Межсетевые экраны какого типа устанавливаются на логической границе информационных систем?	<p>1. Межсетевые экраны типа «А»</p> <p>2. Межсетевые экраны типа «Б»</p> <p>3. Межсетевые экраны типа «В»</p> <p>4. Межсетевые экраны типа «Г»</p> <p>5. Межсетевые экраны типа «Д»</p>
62.	Межсетевые экраны какого типа осуществляют разбор http(s)-трафика между веб-сервером и клиентом?	<p>1. Межсетевые экраны типа «А»</p> <p>2. Межсетевые экраны типа «Б»</p> <p>3. Межсетевые экраны типа «В»</p> <p>4. Межсетевые экраны типа «Г»</p> <p>5. Межсетевые экраны типа «Д»</p>
63.	Что такое модель угроз информационной безопасности?	<p>1. Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независимых от человека.</p> <p>2. Описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.</p> <p>3. Угрозы ИБ АС, вызванные деятельностью человека.</p>
64.	Какие механизмы защиты информации должны обязательно использоваться в криптошлюзах согласно требований руководящих документов?	<p>1. Аутентификации взаимодействующих сторон.</p> <p>2. Криптографическая защита передаваемых данных.</p> <p>3. Подтверждение подлинности и целостности доставленной информации.</p> <p>4. Анализ и перехват трафика для выявления конфиденциальной информации.</p> <p>5. Защите от повтора, задержки и удаления сообщений.</p>
65.	Какие механизмы защиты должен включать сервис для проведения видеоконференций?	<p>1. Защиту передачи аудио и видео по технологии WebRTC.</p> <p>2. Шифрование данных с помощью протоколов TLS, DTLS, AES-128, AES-256.</p> <p>3. Защиту передачи аудио и видео по технологии WebPPC.</p> <p>4. Дополнительное шифрование контента протоколом SRTP.</p> <p>5. Защиту от DDoS-атак.</p>
66.	Какие мероприятия из перечисленных необходимо проводить для решения проблемы несанкционированного доступа к видеоконференцсвязи?	<p>1. Использовать пароль для подключения к конференции и сообщать его участникам по защищенным каналам связи.</p> <p>2. Размещать ссылку и пароль вместе.</p>

		<p>3.Если нет защиты доступа паролем, то следует постоянно менять ссылку приглашения.</p> <p>4.Использовать функцию зала ожидания.</p>
67.	Какие функции из перечисленных выполняют криптошлюзы?	<p>1.Шифрование данных, передаваемых между узлами сети.</p> <p>2.Обнаружение и предотвращение компьютерных атак.</p> <p>3.Управление доступом к данным и ресурсам.</p> <p>4. Все ответы верны.</p>
68.	Что такое криптостойкость?	<p>1.Способность системы радиосвязи противостоять введению в нее неверной информации, а также навязыванию ложных рабочих режимов.</p> <p>2.Способность системы радиосвязи противодействовать раскрытию злоумышленником смысла передаваемой информации.</p> <p>3.Передача ложной информации, специально разработанной для введения злоумышленника в заблуждение, по каналам радиосвязи.</p>
69.	Какие функции из перечисленных выполняет SIEM система?	<p>1.Сбор событий ИБ.</p> <p>2.Контроль каналов коммуникаций, мест хранения информации, действий пользователей на рабочих станциях.</p> <p>3.Анализ поведения пользователей в сети.</p> <p>4.Предоставление пользователю данных об активах, событиях и инцидентах.</p> <p>5.Анализ событий ИБ.</p>
70.	Какие функции из перечисленных выполняет SIEM система?	<p>1.Управление доступом к данным и ресурсам.</p> <p>2.Обработка (корреляция) событий ИБ.</p> <p>3.Создание и управление записями об инцидентах ИБ.</p> <p>4.Отчетность.</p> <p>5.Анализ и перехват трафика компании для выявления конфиденциальной информации.</p>
71.	Какая электронная подпись (ЭП) однозначно подтверждает, что данное электронное сообщение отправлено конкретным лицом?	<p>1.Усиленная неквалифицированная ЭП.</p> <p>2. Усиленная квалифицированная ЭП.</p> <p>3. Простая ЭП.</p> <p>4.Сложная ЭП.</p>
72.	Какие функции из перечисленных выполняют DLP-системы?	<p>1.Контроль рабочего времени сотрудников.</p> <p>2.Обработка (корреляция) событий информационной безопасности.</p> <p>3.Построение отчетов по событиям и инцидентам.</p> <p>4.Работа в территориально распределенной сети.</p>
73.	Какие требования предъявляются к хранению ключевых носителей содержащих электронную подпись?	<p>1.Личные ключевые носители пользователей рекомендуется хранить в электронном виде.</p> <p>2. Личные ключевые носители пользователей рекомендуется хранить в запираемом хранилище.</p> <p>3. Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией.</p>
74.	Какими мерами обеспечивается безопасность резервных копий?	<p>1.Хранение резервных копий в зашифрованном виде.</p> <p>2.Соблюдение мер физической защиты резервных копий.</p> <p>3.Строгая регламентация порядка использования резервных копий.</p>
75.	Какая электронная подпись (ЭП) позволяет не только однозначно идентифицировать отправителя, но и подтвердить, что с момента подписания документа его никто не изменял?	<p>1.Усиленная неквалифицированная ЭП.</p> <p>2. Усиленная квалифицированная ЭП.</p> <p>3. Простая ЭП.</p> <p>4.Сложная ЭП.</p>

Вопросы задания открытого типа для дифференцированного зачета по МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи

1. Как называется процедура распознавания субъекта в процессе регистрации в системе?
2. Как называется процедура проверки подлинности заявленного пользователя, процесса или устройства?
3. Как называется процедура предоставления субъекту определенных прав доступа к ресурсам системы?
4. Какие СЗИ выявляют и соответствующим образом реагируют на средства несанкционированного уничтожения, блокирования, модификации, или нейтрализации СЗИ?
5. Сколько классов защищенности межсетевых экранов по уровням контроля межсетевых информационных потоков определено ФСТЭК?
6. Сколько уровней защиты содержит классификация межсетевых экранов по классам защиты?
7. Какие типы межсетевых экранов определены ФСТЭК России?
8. Где устанавливаются межсетевые экраны типа «А»?
9. Где устанавливаются межсетевые экраны типа «Б»?
10. Где устанавливаются межсетевые экраны типа «В»?
11. Какого типа межсетевые экраны осуществляют разбор http(s)-трафика между веб-сервером и клиентом, и где они устанавливаются?
12. Где подключается система обнаружения вторжений уровня сети и что она контролирует?
13. Где устанавливается система обнаружения вторжений уровня узла и что она анализирует?
14. Какие типы средств антивирусной защиты выделено ФСТЭК?
15. Какие типы средств доверенной загрузки выделено ФСТЭК?
16. Когда возникает ситуация, требующая несколько уровней межсетевых экранов?
17. При каком методе идентификации пользователя первый рубеж - это логин и пароль, второй - специальный код, приходящий по электронной почте?
18. Какие типы средств контроля съемных машинных носителей информации выделяются ФСТЭК?
19. Какие различают типы операционных систем, используемых в целях обеспечения защиты информации?
20. На какие средства вычислительной техники устанавливаются операционные системы типа «А»?
21. На какие средства вычислительной техники устанавливаются операционные системы типа «Б»?
22. Для каких целей предназначены операционные системы типа «В»?
23. Как называют совокупность технических средств, направленных на контроль входа и выхода в помещение с целью обеспечения безопасности и регулирования посещений объекта?
24. При использовании какой модели разграничения доступа указываются полномочия субъекта относительно каждого объекта или сегмента информации?
25. При использовании какой модели разграничения доступа субъект имеет право на чтение только тех объектов, уровень конфиденциальности которых не выше его уровня?
26. Какой стандарт системы аутентификации предоставляет пользователю возможность создания единой учётной записи для аутентификации на множестве интернет-ресурсов, используя услуги третьих лиц?
27. Какой пароль действителен только для одного сеанса аутентификации, действие этого пароля может быть ограничено определённым промежутком времени?
28. Как называют технологию однократного ввода учетных данных для доступа к нескольким системам/приложениям?

29. Какая технология позволяет не только проверять устройства и пользователей на подступах к ресурсам корпоративной сети, но и предотвращать доступ устройств, не соответствующих политике безопасности?

30. Какое средство унифицированного управления угрозами обеспечивает комплексную защиту от сетевых угроз и объединяет в себе множество функций, связанных с обеспечением сетевой безопасности?

31. Как называется процесс оценки подозрительных действий в защищаемой сети, который реализуется либо с помощью анализа журналов регистрации ОС и приложений, либо с помощью анализа сетевого трафика?

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

33. Какие основные группы задач решает шлюз web-безопасности класса SWG?

34. Какова главная задача криптошлюза в сети передачи данных?

35. Какие архитектурные способы установки криптошлюзов в сети являются основными?

36. К каким средствам защиты информации относится криптошлюз?

37. На каких объектах необходимо использовать криптошлюзы по требованиям регуляторов?

38. Какие функции помимо шифрования передаваемого трафика между узлами выполняет криптошлюз?

39. Для каких целей предназначена система мониторинга событий ИБ?

40. Из каких источников данных собирает информацию система мониторинга событий ИБ?

41. Как называют процесс проверки всех событий безопасности, получаемых от антивирусных систем, журналов ОС, сканеров анализа защищенности инфраструктуры, сетевого оборудования?

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

43. Как называют устройство или программное обеспечение для перехвата данных, вводимых с клавиатуры?

44. Какие программы используются для удаленного управления рабочими станциями, выполнения почти любых действий с удаленной системой: передача файлов, наблюдение за действиями пользователя, настройка системы?

45. Какие СЗИ работают внутри периметра безопасности, анализируют учётные записи, права, файлы, их содержимое, доступы и перемещения, выявляют нарушения и исправляют проблемы с хранением данных в компании?

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

47. Какие программные и аппаратные средства используются для обнаружения неавторизованного входа в систему, а также несанкционированных попыток по управлению защищаемой сетью?

48. Как называют единицу информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа?

49. Какая учетная запись имеет больше прав, чем стандартная учетная запись и объем прав таких записей различается в зависимости от организации, должностных обязанностей и используемых технологий?

50. Какая модель описывает потенциального нарушителя безопасности и подходы по определению актуальности угроз и вероятности их наступления с учетом возможностей потенциального нарушителя?

51. Какая целевая продолжительная высокоуровневая атака проводится группировкой профессиональных киберпреступников, зачастую действующих в интересах какого-либо государства?

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

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

54. Как называют технологию поиска, аккумуляции и анализа данных, собранных из доступных источников в интернете?
55. Какие средства защиты устанавливают между общедоступной сетью (такой, как Internet) и внутренней?
56. Какую функцию выполняет межсетевой экран?
57. Для чего нужно контролировать и регулировать доступ пользователей внутренней сети к ресурсам общедоступной сети?
58. На какие группы можно разделить все межсетевые экраны по способу их реализации?
59. Какая VPN защищает данные, передаваемые между узлами корпоративной сети (но не сетями) и обычно реализуется для узлов, находящихся в одном сетевом сегменте?
60. Что такое Next-generation firewall (NGFW)?
61. Для каких целей используются прокси-серверы?
62. Для каких целей используются средства или модули доверенной загрузки (СДЗ или МДЗ)?
63. Для чего используют сканеры уязвимостей?
64. Для чего используют системы защиты от утечек информации (DLP)?
65. Что такое SIEM системы?
66. Кто является оператором персональных данных (ПДн)?
67. Кто является субъектом персональных данных (ПДн)?
68. На какие категории делятся персональные данные?
69. Какие данные относятся к биометрическим персональным данным?
70. Какие данные относятся к специальным персональным данным?
71. Какие данные относятся к общедоступным персональным данным?
72. Какие данные относятся к иным персональным данным?
73. Какие типы актуальных угроз учитываются при работе с ИСПДн?
74. Для чего проводят аудит информационной безопасности?
75. Являются ли равнозначными понятиями служебная и профессиональная тайна?

Составил:

Преподаватель Е.М. Грубник