**Критография 1**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Уровен сложности** | **Вопросов на тестирование** | **Правилъный ответ** | **Алътернативный ответ** | **Алътернативный ответ** | **Алътернативный ответ** |
| *1* | Сколько основных составляющих у информационной безопасности? | 3 | **2** | **4** | **5** |
| **1** | Статус, предоставленный данным и определяющий требуемую степень их защиты – это: | Конфиденциальность информации | Целостность информации | Доступность | Компактность |
| **1** | Свойство, гарантирующее беспрепятственный доступ к защищаемой информации для законных пользователей – это: | Доступность | Конфиденциальность информации | Целостность информации | Компактность |
| **1** | Меры по предотвращению утраты и утечки конфиденциальной информации и утраты защищаемой открытой информации  – это: | Защита информации | Информационная безопасность | Информационная война | Уязвимость информации |
| **1** | Свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения – это: | Целостность информации | Конфиденциальность информации | Доступность | Компактность |
| **1** | К чему приведет информатизация общества? | К единому информационному пространству | К единому телефонному пространству | К единому пространству информационной безопасности | К единому сервисному пространству |
| **1** | Информационное оружие– это: | Средства уничтожения, разрушения или кражи массивов информации, средства уничтожения систем защиты | Средства разработки, изменения или ускорения информационного пространства | Разработка средств наблюдения или кражи | Средство поддержки системы защиты, средство усиления системы защиты |
| **1** | Разработку каких программ на сегодняшний день финансируют руководители некоторых государств? | Кибер-программ | Windows-программ | Достоверных программ | Новых программ |
| **1** | Что из ниже перечисленного можно отнести к атакующему информационному оружию в настоящее время? | Компьютерные вирусы и логические бомбы | Компьютерные программы и логические бомбы | Компьютерные подсистемы и логические билоги | Компьютерные программы и игры |
| **1** | От каких воздействий необходимо защищать информацию? | От несанкционированного доступа к информации, от повреждения или уничтожения информации | От законного доступа к информации, от обработки или продажи информации | От законного доступа к информации, от обработки или использования информации | От соответствующего доступа к информации и передачи ее по сети |
| **1** | Какой подход к безопасности позволяет, с помощью правильно спроектированных и хорошо управляемых процессов и средств, в реальном масштабе времени контролировать, определять риски безопасности и реагировать на них? | Адаптивный | Высокоскоростной | Альтернативный | Реальный |
| **1** | Как определяется стоимость информации в информационной безопасности? | Величиной возможного ущерба в случае нарушения информационной безопасности | Важностью информации для пользователя в случае нарушения информационной безопасности | Защищённостью информации от незаконного ознакомления, преобразования и уничтожения | Ценностью аппаратных и программных средств для хранения, обработки и передачи информации |
| **1** | Кто из знакомых с внутренним порядком в организации, может нанести ей ущерб с большой эффективностью? | Обиженные сотрудники | Администраторы | Хакеры | Все сотрудники |
| **1** | Выберите правильное название компьютерной преступности? | Виртуальные жулики | Компьютерные программы | Сетевые вирусы | Продавцы компьютеров |
| **2** | В целом каким рискам может подвергаться компьютерная среда предприятия? | 1-потеря или изменение данных, 2-остановка сервиса | 1-копирование данных, 2-вирусные атаки | 1-сетевые атаки, 2-ошибки программ | 1-потеря данных пользователя, 2-блокировка системы |
| **2** | Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации – это | Угроза | Уязвимость | Атака | Целостность |
| **2** | Какие типы ошибок пользователей, операторов, администраторов и других, относятся к опасным (с точки зрения величины угрозы) и часто повторяющимся угрозам | Непреднамеренные ошибки | Непродуманные ошибки | Неправильные ошибки | Случайные ошибки |
| **2** | Какое понятие тесно связанно с понятием угрозы безопасности? | Уязвимость компьютерной системы | Надежность компьютерной системы | Эффективность защиты информации | Антивирусные программы |
| **2** | Какие из перечисленных угроз относятся к случайным? | Сбои и отказы технических средств | Несанкционированный доступ к информации | Вредоносные программы | Традиционный шпионаж и диверсии |
| **2** | Какие из перечисленных угроз относятся к преднамеренным? | Несанкционированная модификация структур | Стихийные бедствия и аварии | Сбои и отказы технических средств | Ошибки пользователей и технического персонала |
| **3** | Какой смысл имеет термин «информационной войны» введенный военными? | Опасная и беспощадная деятельность, связанная со смертельными и разрушающими военными действиями | Устрашающая людей деятельность, связанная с военными действиями | Разрушающая деятельность, связанная с могуществом военной сферы | Деятельность связанная с разрушающими действиями военной сферы |
| **3** | Укажите основные типовые дистанционные атаки на информацию в сети? | 1- анализ сетевого трафика, 2 – введение ложных объектов сети, 3 – введение ложного маршрута, 4 – атаки, типов отказа обслуживание | 1-подключение к открытому порту компьютера, 2- законное использование из сети, 3-введение ложного маршрута, 4-атаки на управление системой | 1- подключение к компьютерным системам, 2- законное использование из сети, 3- введение ложного маршрута, 4-вирусные атаки | 1- законное использование из сети, 2- введение ложного маршрута, 3- Атаки на эффективность использования сети |
| **3** | По какому показателю занимает второе место в информационной безопасности несанкционированный доступ и фальсификация информации? | По величине ущерба | По значимости информации | По объему информации | По объему дохода |
| **3** | Какие угрозы называются пассивными? | Угрозы, которые при реализации ничего не меняют в структуре и содержании информации (например, копирование) | Угрозы, которые никогда не реализуются | Угрозы, которые не нарушают информационной безопасности | Угрозы, связанные с техническими средствами |
| **1** | Какой доступ к информации называется санкционированным? | Не нарушающий установленные правила разграничения доступа | Нарушающий установленные правили разграничения доступа | Не нарушающий целостность информации | Не нарушающий конфиденциальность информации |
| **1** | Какой доступ к информации называется несанкционированным? | Какой доступ к информации называется несанкционированным? | Не нарушающий целостность информации | Не нарушающий конфиденциальность информации | Не нарушающий установленные правила разграничения доступа |
| **1** | Когда можно перехватить информационные пакеты? | При передаче через каналы связи | При передачи в память | При включении компьютера | При копировании данных |
| **2** | Что понимается под маршрутом при передаче данных? | Последовательность сетевых узлов | Повреждение сетевых узлов | Процесс последовательного соединения сетевых устройств | Процесс дистанционного определения пользователя |
| **2** | Покажите причину незащищённости информации в сети от основных удаленных типовых атак | Не совершенность интернет-протоколов | Низкая скорость каналов связи | Повышение объемов передаваемой информации в сети | Повышение квалификации нарушителей |
| **3** | В каких ситуациях с помощью специальных сканер программ можно перехватить пакет в котором указаны имя и пароль пользователя? | Когда незашифрованные пароли | Когда видно это пакет | Когда пакет записан | Из-за ошибок в программе |
| **1** | Каким видам рисков подвергается компьютерная среда предприятия? | Потеря или изменение данных, остановка сервиса | Распад сетевых узлов | Появление рисков, не приводящих к серьезным нарушениям | При обмене данных между компьютерами пользователей |
| **1** | Кто может осуществлять вторжение в компьютерные сети на сегодняшний день? | Хакеры, крэкеры, компьютерные пираты | Пользователи, сетевые администраторы | Пользователи удаленного доступа, процесс определения атаки | Потеря или изменение данных, остановка сервиса |
| **2** | Укажите тип распределенной атаки, который вызывает отказ в обслуживании? | DDOS (Distributed Denial of Service) атаки | Сетевые атаки | Программные атаки | Вирусные атаки |
| **2** | На какие категории можно разделить нарушителей информационной безопасности? | 1- любители приключений. 2- идейные хакеры, 3-хакеры-профессионалы, 4- ненадежные сотрудники | 1- злоумышленники, 2- идейные хакеры , 3- хакеры-профессионалы, 4- предатели | 1-злоумышленники, 2- программисты, 3- хакеры, 4-предатели | 1-пользователи , 2-сотрудники, 3-хакеры,4- предатели |
| **2** | Нарушитель информационной безопасности, молодой , в большинстве случаев студент или учащийся старших классов, обычно не имеющий плана атаки – это: | Любитель приключения | Идейный хакер | Профессиональный хакер | Ненадежный сотрудник |
| **2** | Кто не относится к категории профессиональных хакеров? | Любитель приключений | Группа хакеров стремящаяся получить прибыль бесплатно | Промышленные шпионы | Уголовные группы, с политическими целями |
| **3** | Профессиональные хакеры – это: | Группа хакеров стремящиеся к политическим целям, и получению бесплатной прибыли | Группа хакеров стремящиеся взломать и разрушить сети | Группа хакеров стремящиеся взломать и украсть информацию | Группа хакеров стремящиеся взломатьинформацию и предлагающие поделится ею |
| **3** | Нарушитель информационной безопасности, имеющий точный план действий, нацеленный на определенные ресурсы, и обычно реализуемый в несколько этапов – это: | Хакер профессионал | Любитель приключений | Идейный хакер | Ненадежный сотрудник |
| **3** | Кто своими действиями создает проблемы равные (или превышающие) промышленный шпионаж? | Ненадежный сотрудник | Хакер-профессионал | Любитель приключений | Идейный хакер |
| **3** | Где определяются национальные и корпоративные интересы, принципы обеспечения информационной безопасности и пути поддержки, а также приводятся задачи по их реализации? | В концепции | В стандартах | В указах | В приказах |
| **3** | На основе чего разрабатывается стратегия информационной безопасности и архитектура системы защиты? | Концепция информационной безопасности | На основе стандартов | На основе указов | На основе приказов |
| **1** | Спам - это: | Нежелательная корреспонденция рекламного характера | Зараженные рекламные ролики | Нежелательная корреспонденция, отправляющая почтовые сообщения | Компьютерные вирусы рекламного характера |
| **1** | Концепция информационной безопасности – это: | Официальные взгляды на проблемы информационной безопасности | Совокупность атак на информацию | Порядок пользования информацией | Взгляды на разработку и обработку информации |
| **1** | Сколько этапов включает в себя создание концепции информационной безопасности? | 3 этапа | 4 этапа | 5 этапов | 6 этапов |
| **1** | Концепция защиты информации – это: | Официально принятая система взглядов на проблему информационной безопасности | Совокупность атак на информацию | Совокупность использования к информации | Взгляды на создания и обработки информации |
| **1** | Сколько этапов при разработке концепции информационной безопасности? | 3 этап | 4 этап | 5 этап | 6 этап |
| **2** | Укажите цели интереса компьютерных преступников. | Корпоративные компьютерные сети | Конкретный пользователь | Запоминающие устройства | Системный администратор |
| **2** | Что осуществляется на первом этапе разработки концепции информационной безопасности? | Определение стоимости защищаемых объектов | Анализ преднамеренных действии злоумышленника | Оценка надежности средств защиты информации | Ускорение проектирования системы |
| **2** | Укажите цель которая привлекает компьютерных злоумышленников? | Корпоративные компьютерные системы | Одинокие пользователи | Средства хранения данных | Системный администратор |
| **3** | Что осуществляется на втором этапе разработки концепции информационной безопасности? | Анализ возможных действий взломщика | Ускорение проектирования системы | Определение ценности защищаемого объекта | Оценка надежности средств защиты информации |
| **3** | Что осуществляется на третий этапе разработки концепции информационной безопасности? | Оценка надежности средств защиты информации установленных в объекте | Ускорение проектирования системы | Анализ возможных действий взломщика | Определение ценности защищаемого объекта |
| **1** | Укажите наиболее частое состояние нарушения информационной безопасности | Несанкционированный внутренний доступ в сети | Использование ошибки в проектировании | Подключение к ресурсам внешней сети | Подключение к беспроводной сети |
| **1** | Укажите основное свойство обшей стратегии информационной безопасности | Исследование системы безопасности | Определение объектов системы | Оптимизация управления системы | Процесс сканирования системы |
| **1** | Что не относится к организационным мерам? | Установка лицензированных антивирусных программ | Организация надежного пропускного режима и контроля посетителей | Надежная охрана комнат и территории | Меры, реализуемые при подборе кадров |
| **2** | На основе чего разрабатывается стратегия информационной безопасности и архитектура системы защиты? | На основе концепции информационной безопасности | На основе обстоятельств во время проектирования системы | На основе упрощения устройств информационной системы | На основе попыток взлома системы |
| **3** | В каком порядке должны быть средства противодействия атакам? | Соответствие защиты полной эшелонированной концепции, в центре средств противодействия должен быть защищаемый объект | Отдельное место для объекта и его охраны | Близкое расположение противодействующих средств | При последовательном соединении запоминающих устройств |
| **3** | В каком ответе правильно показано проектирование и этапы реализации эффективной защиты в информационной системе? | Анализ рисков, реализация политики безопасности, поддержка политики безопасности | Определение защищаемых объектов, анализ атак | Контроль пользователей и сети, построение защиты сети | Анализ рисков, разработка мер по проектированию |
| **1** | Что относится к организационно-административным мерам? | Подбор сотрудников, охрана компьютерных систем | Проектирование системы, обучение персонала | Разработка системы, контроль сети | Установка связи, контроль сети |
| **1** | Что относится инженерно-техническим мерам? | Защита от несанкционированного доступа к системе, резервирование важных компьютерных подсистем, обеспечение защиты от диверсии и кражи | Резервирование важных компьютерных подсистем, продажа, фальсификации | Несанкционированный доступ к системе, фальсификация важных сведений, защита от отказов | Запрет доступа к системе, определение сетевых преступников |
| **2** | Как расценивается кража информации связанная с потерями материальных и духовных богатств? | Расценивается как уголовное дело | Расценивается как поощрение | Считается нарушением | Считается борьбой между группами |
| **2** | Что определяется в первую очередь при разработке политики информационной безопасности? | Защищаемый объект и его функции | Существующие средства защиты | Требования к системе защите | Сроки организации системы защиты |
| **2** | Какое обеспечение не разрешает доступ к конфиденциальной информации? | Организационное | Правовое | Финансовое | Прикладное |
| **3** | Укажите меры обеспечивающие информационную безопасность? | 1-правовые, 2-организационно-административные, 3-инженерно-технические | 1-нравственные, 2-организационно-административные,3-физические | 1-программные, 2-организационно-административные, 3-правовые | 1-аппартаные, 2-технические, 3-правовые |
| **3** | Определите правовое обеспечение информационной безопасности. | Законы, акты, нормативно-правовые документы, правила, руководства, комплекс инструкций | Правила,руководства, архитектура системы, квалификация сотрудников | Правила,руководства, структура системы, программное обеспечение | Проектирование системы защиты, методы контроля |
| **3** | Что определяют общие принципы политики информационной безопасности? | Подход к безопасности в интернете | Набор средств защиты информации | Временные нормы реализации безопасности | Этапы защиты информации |
| **3** | Что определяют конкретные правила работы политики информационной безопасности? | Разрешения и запреты | Набор средств защиты информации | Временные нормы реализации безопасности | Этапы защиты информации |
| **1** | В общем случае, сколько подсистем включают в себя меры защиты? | 4 | 5 | 6 | 7 |
| **1** | Сколько классов защиты от несанкционированного доступа к информации определены? | 7 классов | 8 классов | 10 классов | 11 классов |
| **1** | Каким этапом является поддержка политики безопасности? | Самым важным этапом | Не важным этапом | Финансированным этапом | Альтернативным этапом |
| **2** | Что реализуется в первом этапе проектирования и реализации системы безопасности? | Анализируется уязвимые элементы компьютерной сети | Анализируются элементы операционной системы | Анализируются ошибки пользования | Анализируется сетевое оборудование |
| **2** | Укажите этапы проектирования и реализация системы защиты? | 1-анализ рисков и угроз 2- реализация политики безопасности 3- поддержка политики безопасности | 1- анализ пользований 2-подбор сотрудников безопасности 3-перепроектирование сети | 1-поиск недостатков сети2-подбор сотрудников безопасности 3-пересмотрполитики | 1- обновление программ 2- подбор сотрудников безопасности |
| **3** | В общем случае какие подсистемы включают в себя меры защиты? | 1-управление доступом 2-протоколирование 3-криптография 4-обеспечение целостности | 1-управление системой 2-мониторинг 3-криптография | 1-нарушение доступности 2-протоколирование | 1-Копирование 2-протоколирование 3-определение атаки |
| **3** | Из чего должна состоять система для получения класса защищенности? | 1-руководство администратора по системе, 2-руководство пользователя, 3- тестовые конструкторские документы | 1-общие сведения о системе, 2-информация пользователей, 3- мониторинг системы | 1-проверка состояния системы, 2-полная информация о программе | 1-оценивание системы, 2-определение обязанностей администратора |
| **3** | На каком этапе проектирования системы защиты анализируется уязвимые элементы, определяются и оцениваются угрозы, для обеспечения эффективной защиты информации в компьютерных сетях? | При анализе опасности | При реализации политики безопасности | При поддержке безопасности | При построении компьютерной сети |
| **3** | Какой этап проектирования системы защиты начинается расчетом финансовых затрат и выбором соответствующих средств для задач реализации политики безопасности для обеспечения эффективной защиты информации в компьютерных сетях? | Реализация политики безопасности | Оценка опасности | Поддержка политики безопасности | Построение компьютерной сети |
| **3** | Какая служба обеспечивает защиту от возможности открытия информационной среды, несанкционированного доступа к информации и кражи в сети передачи данных? | Обеспечение конфиденциальности | Информационное обеспечение | Техническое обеспечение | Обеспечение стойкости |
| **1** | Чему посвящена первая часть «Оранжевой книги»? | Комментарию конфигурации сети | Введению | Безопасности | Мероприятиям по безопасности |
| **1** | Чему посвящена вторая часть «Оранжевой книги»? | Описываются сервисы безопасности важные для конфигурации сети | Комментарию конфигурации сети | Посвященавведению | Посвящена мероприятиям |
| **1** | Совокупность законодательных актов, нормативно- правовых документов, правил, инструкций подлежащие обязательному выполнению в системе защиты информации – это: | Правовое обеспечение информационной безопасности | Организационное обеспечение информационной безопасности | Методическое обеспечение информационное безопасности | Прикладное обеспечение информационной безопасности |
| **2** | Какие нормативы включены в правовую основу информационной безопасности? | Международные и национальные правовые нормы | Организационные и международные нормы | Традиционные и корпоративные нормы | Нормы государственных и негосударственных организаций |
| **2** | Что включает в себя правовое обеспечение информационной безопасности любого государства? | Международные и национальные правовые нормы | Международные стандарты | Законы, относящиеся к информационной безопасности любого государства | Нормы международных организаций |
| **3** | Укажите стандарт шифрования информации в США? | DES(DataEncryptionStandart) | RSA (Rivest, Shamir иAdleman) | AES (AdvancedEncryptionStandart) | Не используется определенный стандарт |
| **3** | К каким мерам относится разработка нормативов определяющих ответственность за компьютерные преступления, защиту авторских прав программистов и совершенствование уголовных и гражданских законодательств, а также судебных процессов? | Правовым | Организационно-административным | Инженерно-техническим | Финансовым |
| **1** | В чем состоит общая цель методов обеспечения информационной безопасности, и средств защиты информации? | Что, от чего и как защищать? | Когда, как защищать? | Компьютерная информация, база данных | Обеспечение доступности, криптографическая зашита информации |
| **2** | Кто решает проблемы задачи поддержки правильной конфигурации сетевой ОС? | Администратор сети | Пользователь сети | Руководитель организации | Оператор |
| **2** | К каким мерам относится охрана компьютерных систем, подбор кадров, недопущение выполнения особо важных работ одним человеком? | Организационно-административным | Правовым | Инженерно-техническим | Финансовым |
| **3** | Что из приведённогоявляется важным при разработке надежного механизма защиты информации? | Организационные меры | Массовые меры | Антивирусные программы | Квалификация пользователей |
| **3** | К каким мерам относится защита от несанкционированного доступа к компьютерным системам, резервирование важных компьютерных систем, защита от кражи и диверсии, обеспечение резервного электропитания, разработка и реализация специальных программных и аппаратных средств? | Инженерно-техническим | Финансовым | Организационно-административным | Правовым |
| **1** | В чем заключается цель шифрования информации? | Шифровать и скрывать смысл конфиденциальной информации | Сжатие и архивирование информации | Собрать и продать кодированную информацию | Передача информации |
| **1** | Какой процесс понимается под шифрованием информации? | Преобразование открытой информации в закрытую с помощью ключа | Сборкодированных данных | Процесс преобразования информации | Последовательность процессов |
| **1** | Какой процесс понимается под дешифрованием информации? | Преобразование закрытой информации в открытую с помощью ключа | Распространение хранимой секретных данных | Несанкционированный доступ к информации в сети | Незаконное подключение и пользование сетевыми ресурсами |
| **2** | На какие два вида делятся криптосистемы? | 1-симетричная криптосистема (один ключ),2- ассиметричная криптосистема (два ключа) | 1- перемещение места 2-распределение ключей (двух ключевой) | 1-способ гаммирования, 2-обмен ключами | 1-Шифрование через сеть, 2-Распространение ключей |
| **3** | Пароль – это: | Информация которую знает пользователь, а также тот с кем он обменивается информацией | Имя пользователя | Ключ шифрования информации | Носитель информации |
| **1** | Какая информация используется для шифрования и дешифрования в симметричных криптосистемах? | Один ключ | Электронная цифровая подпись | Идентификатор пользователя | Открытый ключ |
| **1** | При шифровании какой информации удобно симметричное шифрование? | При хранении информации для себя | Открытая информация | При обработке информации | Личная информация |
| **1** | В чем заключаются неудобства симметричного шифрования? | Необходимость обмена секретным ключом | Конфиденциальность ключей | Большая размерность ключей | Большая длительность шифрования |
| **3** | Какие алгоритмы симметричного шифрования используются при формировании и проверке электронной цифровой подписи? | RC4, RC2 и DES, Triple DES | Triple DES, RSA иDiffi-Xelman | RC4, RC2 иDiffi-Xelman | RSA и Diffi-Xelman |
| **1** | С помощью какого стандарта производится формирование сертификатов открытых ключей? | X.509 | X.9.45 | X.500 | X.400 |
| **2** | Какая информация используется для шифрования и дешифрования в асимметричных криптосистемах? | Два ключа | Один ключ | Электронная цифровая подпись | Идентификатор пользователя |
| **3** | В каком ответе неправильно показаны алгоритмы Xesh –функции? | DES, RSA | Гаммирование, цезарь | Kerberos | FTP, TCP, IP |
| **1** | От чего зависит возможность подделки ЭЦП пользователя в системе электронной цифровой подписи? | Нельзя подделать | От длины ключа | Нет проблем с подделкой | От конфиденциальности подписанного текста |
| **2** | На основании каких алгоритмов разрабатывается электронно-цифровая подпись ? | El-Gamal, RSA | Kerberos | AES (AdvancedEncryptionStandart | DES(DataEncryptionStandart) |
| **2** | В каком ответе неправильно приведены преимущества электронной цифровой подписи? | Гарантирует доступность подписываемого текста | Удостоверяет что подписываемый текст исходит от лица, поставившего подпись | Не дает самому лицу возможность отказаться от обязательств, связанных с подписанным текстом | Гарантирует целостность подписанного теста |
| **2** | Какую информацию не включает в себя электронная цифровая подпись? | Информацию о получатель электронного документа | Дату подписи | Информацию о лице, подписавшем файл | Идентификатор подписавшего |
| **3** | Какие алгоритмы асимметричного шифрования используются при формировании и проверке электронной цифровой подписи? | RSA и Diffi- Xelman | RC2 и MD5 | RC4и El-Gamal | RSA и DES |
| **3** | Как называется относительно небольшое количество дополнительной цифровой информации, передаваемое вместе с подписываемым текстом? | Электронная цифровая подпись | Ключ шифрования | Электронный цифровой пароль | Идентификатор пользователя |
| **1** | Какие полномочия даёт авторизация при доступе к системе? | Определяет область действия субъекта и используемые им ресурсы | Дает возможность пользования ресурсами | Даёт возможность изменять ресурсы | Определяет ресурсы не доступные субъекту |
| **1** | Самый часто используемая основа аутентификации? | Пароль | Биометрические параметры | Смарт карты | Электронная цифровая подпись |
| **1** | Процедура распознавания пользователя по его идентификатору, присвоенному данному пользователю ранее – это: | Идентификация | Аутентификация | Авторизация | Администрирование |
| **1** | Укажите правильную последовательность названий процессов? | Идентификация, аутентификация, авторизация, администрирование | Аутентификация, идентификация, авторизация, администрирование | Авторизация, администрирование, идентификация, аутентификация | Идентификация, авторизация, администрирование, аутентификация |
| **2** | Какие данные используются при идентификации пользователя? | Идентификатор (имя) | Номер телефона | Пароль | Фотография |
| **2** | Какие данные используются при аутентификация пользователя? | Пароль | Имя | Пол | Номер телефона |
| **2** | Процедура предоставления определённых полномочий и ресурсов субъекту – это: | Авторизация | Подтверждение подлинности | Аутентификация | Идентификация |
| **2** | Процедура предоставления определённых полномочий и ресурсов субъекту – это: | Авторизация | Подтверждение подлинности | Подтверждение подлинности | Подтверждение подлинности |
| **3** | Регистрация действий пользователя и его попыток пользования ресурсами в сети – это: | Администрирование | Аутентификация | Идентификация | Сертификация |
| **3** | Процедура проверки подлинности представившегося пользователя, процесса или устройства – это: | Аутентификация | Идентификация | Администрирование | Авторизация |
| **3** | Покажите основные возможные атаки на протоколы аутентификации. | Maskarad (подмена сторон аутентификационного обмена), вынужденная задержка, атака с выборкой текста | Атаки типа отказа в обслуживании | Атаки выводящие из строя компьютерную систему | АтакиDOS и DDOS |
| **1** | Динамический пароль – это: | Пароль, используемый один раз | Пароль, используемый много раз | Имя пользователя | Сертификат |
| **2** | Пароль, используемый один раз – это: | Динамический пароль | Статический пароль | Электронная цифровая подпись | Код пользователя |
| **3** | Аутентификация на основании уникальных характеристик человека - это: | Биометрическая аутентификация | Аутентификация на основании паролей | Аутентификация на основании биографии | Аутентификация на основании смарт-карты |
| **3** | Преимущества методов биометрической аутентификации? | Уникальность биометрических признаков | Одноразовое использование | Возможность изменения биометрических признаков | Простота процесса аутентификации |
| **1** | Технология межсетевого экранирования – это: | Выполнение функций фильтра и защиты между внутренней и внешней сетью | Выполнение функции преобразования информации между внутренней и внешней сетью | Защита законных пользователей | Управление доступом из ненадежной сети |
| **1** | На сколько групп делятся защищенные виртуальные частные сети | 3 | 4 | 5 | 6 |
| **2** | Основная функция межсетевого экрана – это: | Управляет доступом к информации между надежной и ненадежной сетью | Определение сетевых атак | Запрещение трафика | Соединение и отсоединение потока сообщений в сети |
| **2** | В чем заключается основная функция межсетевого экрана? | Защита внутренней сети предприятий от вторжений из сети Интернет | Защита локальной сети предприятия от атак из корпоративной сети Интранет | Отключение внутренней сети предприятия от глобальной сети Интернет | Ограничение доступа к сети Интернет |
| **3** | Что разделяет общую сеть на две и более части и реализует набор правил, определяющих условия прохождения пакетов с данными через границы областей сети? | Межсетевой экран | Средства анализа защищённости | Средства обнаружения атаки (IDS) | Антивирусная программа |
| **3** | Укажите основные типы межсетевых экранов? | Прикладной шлюз, шлюз сеансового уровня, экранирующий маршрутизатор | Прикладной шлюз, шлюз сеансового уровня, шлюз физического уровня | Прикладной шлюз, шлюз физического уровня,экранирующий маршрутизатор | Шлюз физического уровня,экранирующий маршрутизатор, анализирующий маршрутизатор |
| **1** | Сколько типов протоколов используется при реализации механизмов тунеллирования? | 3 | 4 | 6 | 7 |
| **1** | В состав какой сети, с организационной точки зрения, входит межсетевой экран? | Защищаемой сети | Глобальной сети | Корпоративной сети | Локальной сети |
| **2** | Укажите протоколы тунеллирования канального уровня модели OSI. | PPTP, L2F и L2TP | DES и RSA | RSA и DES | DES и Triple DES |
| **2** | Что является необходимым условием обеспечения информационной безопасности внутренней сети для большинства коммерческих организаций? | Установка межсетевого экрана | Выполнение организационных работ | Отключение от глобальной сети | Использование оптоволоконных каналов связи |
| **3** | Какой транспортный протокол доставляющий данные может быть использован в качестве протокола-«пассажира» в локальных сетях филиалов одной организации? | IPX | TCP | FTP | PPTP |
| **1** | По скольким признакам классифицируются защищенные виртуальные частные сети? | 3 | 4 | 2 | 5 |
|  | Какое соединение используется в виртуально защищённом туннеле? | Соединение, проведенное через открытую сеть | Соединение, обеспечивающее высокую скорость | Соединение, проведенное через защищенную сеть | Соединение, проведенное через экранированные каналы связи |
| **2** | Укажите группы VPN по технической реализации? | VPN на основе маршрутизаторов, VPN на основе межсетевых экранов, VPN на основе программного обеспечения, VPN на основе специализированных аппаратных средств | VPN с удаленным доступом, межкорпорационный VPN | VPNс удаленным доступом, межгосударственный VPN | Межкорпорационный VPN, VPN скрывающий стороны при взаимном обмене |
| **2** | С какой целью введено понятие «виртуальный» в концепции VPN? | Обозначения временности соеденения между двумя узлами | Обозначение невидимости соединения между двумя узлами | Обозночения оптоволокна | Обозначение постоянства соединения между двумя узлами |
| **3** | Определите задачи защищённости информации в процессе передачи по туннели VPN... | Аутентификация взаимодействующих сторон, криптографическаязащита передаваемых данных | Авторизация взаимодействующих сторон,криптографическаязащита передаваемых данных | Идентификация взаимодействующих сторон | Защита взаимодействующих сторон |
| **3** | Основное преимущество виртуального защищеного туннеля - это: | Высокая труднодоступность для внешних пассивных и активных наблюдателей | Легкодоступность для внешних пассивных и активных наблюдателей | Высокое удобство использования для внешних пассивных и активных наблюдателей | Недоступность для внешних пассивных и активных наблюдателей |
| **1** | Укажите протоколы тунеллирования канального уровня модели OSI? | PPTP, L2F и L2TP | IP, PPP и SSL | VPN, IPX и NETBEU | GRE, IPSec и DES |
| **2** | Какой протокол используется для аутентификации в системах обмена ключевых слов предназначенный для установки защищенного канала? | ПротоколKerberos | ПротоколChap | ПротоколPPP | ПротоколIPsec |
| **3** | Какие алгоритмы и криптосистемы используются при распределении ключа шифрования в межсетевых экранах BorderManager? | RSA и Diffi-Xellman | RSA и RC2 | RSA и DES | RC2 и Diffi-Xellman |
| **3** | Что используется при безопасной передаче данных через открытую сеть в VPN? | Инкапсуляция и туннелирование | Идентификация и аутентификация | Межсетевые экраны | Электронные цифровые подписи |
| **2** | В каком ответе неправильно показаны основные схемы использования IPSec? | шлюз-хост” | шлюз- шлюз” | “хост - шлюз” | “хост- хост” |
| **3** | На какой логике основан процесс туннелирования? | «Конверт в конверте» | Шифрование «конверта» | Безошибочная передача | Конфиденциальность и целостность |
| **3** | Какие функциональные требования должны обеспечивать возможность определения подлинности пользователей участвующих в процессе передачи данных? | Аутентификация пользователей | Идентификация пользователей | Обеспечение конфиденциальности | Аудит |
| 1 | Укажите вредоносные программы | Логические бомбы и компьютерные вирусы | Не лицензированные программы и устройства | Сетевые карты и программы | Программы сети интернет |
| **1** | Из каких основных этапов состоит жизненный цикл вирусов? | 1-хранение 2-выполнение | 1-создание 2-удаление | 1-распространение 2-изменение | 1-копирование 2-запуск |
| **1** | Какие вирусы считаются опасными? | Приводящие к серьёзным последствиям при работе компьютера | Не приводящие к серьёзным последствиям при работе компьютера | Большие вирусы | Пассивные вирусы |
| **1** | Какой процесс осуществляет поиск уязвимостей сети в адаптивной безопасности? | Анализ защищенности | Оценка рисков | Определение атаки | Расчет стойкости |
| **2** | Какую задачу выполняют загрузочные вирусы при загрузки системы? | Программный код который завладевает управлением | Восстановление связи с программами при загрузки | Проверка ошибок системы при загрузки | Вывод из строя управления при загрузки |