

РГП на ПХВ«Костанайский государственный университет им. А. Байтурсынова»

Вопросы и ответы для мультимедийного задания по проверке знаний студентов по курсам «**Защита информации**», «**Методы и средства защиты компьютерной информации**».

Составлены профессором кафедры вычислительной техники и программирования ФГБОУ ВО «Магнитогорский государственный технический университет» Ячиковым Игорем Михайловичем

Костанай 2019 г

|  |  |
| --- | --- |
| Вопрос **1**  Выберите один или несколько ответов | К причинам случайной потери данных при фарс-мажорных обстоятельствах относятся… |
| ● пожары;  ○ сбой работы процессора или памяти компьютера;  ● удар молнии в электросеть;  ○ ошибки в программах;  ○ потерянный программистом ключ к данным; |
| Вопрос **2**  Выберите один ответ или несколько ответов | Конфиденциальность информации гарантирует… |
| ● доступность информации кругу лиц, для кого она предназначена;  ○ защищенность информации от потери;  ○ защищенность информации от фальсификации;  ○ доступность информации только автору;  ● доступность информации законным пользователям. |
| Вопрос **3**  Выберите один или несколько ответов | Какие задачи могут преследовать злоумышленники? |
| ● Ознакомление, получение информации;  ○ Обеспечение целостности данных при передаче информации;  ● Модификация информации;  ● Подмена информации;  ○ Обеспечение конфиденциальности информации.  ● Личное обогащение;  ○ Повышение своей квалификации. |
| Вопрос **4**  Выберите один ответ | Что входит в классификацию вредоносных программ по степени их опасности? |
| ○ скрывающие свое наличие в системе;  ○ полиморфные;  ○ макровирусы;  ● безобидные;  ○ невидимые. |
| Вопрос **5**  Выберите один ответ или несколько ответов | Как обеспечивается защита от внутренних угроз корпоративной безопасности? |
| ○ С помощью специализированного антивирусного программного обеспечения;  ● Системными административными мероприятиями;  ● Разграничение сотрудникам организации доступа к данным;  ● Комплексными мероприятиями внутреннего контроля и работы с конкретными людьми по минимизации рисков;  ○ Периодическая переустановка ПО. |
| Вопрос **6**  Выберите один ответ | Чему равна длина ключа в шифре ГОСТ 28147-89 (бит)? |
| ○ 56  ○ 64  ○ 128  ● 256  ○ 512 |
| Вопрос **7**  Выберите один или несколько ответов | Что относится к *внешним* факторам, негативно влияющим на качество функционирования программных средств? |
| ● Сбои и отказы аппаратуры вычислительных средств;  ○ Низкая эффективность методов и средств защиты данных;  ○ Алгоритмические ошибки разработки программного обеспечения;  ● Искажения и потери информации при ее передаче. |
| Вопрос **8**  Выберите один ответ | Переменные *a=*–7и *b*=5 описаны как int32. Чему будет равно значение выражения  **1–2\*((unsigned)a\*b)>>31** ? |
| ○ – 69  ● –1  ○ 1  ○ 71 |
| Вопрос **9**  Выберите один или несколько ответов | Какие алгоритмы для нахождения простых чисел используют малую теорему Ферма? |
| ● Лемана;  ○ Решето Эратосфена;  ● Рабина-Миллера;  ○ Эль-Гамаля;  ○ Фейштеля. |
| Вопрос **10**  Выберите один ответ | В каком случае построение алгоритма цифровой подписи не требует наличия в системе третьего лица – посредника, хранящего дополнительную информацию об участниках? |
| ○ при шифровании с помощью симметричного алгоритма;  ○ при шифровании с помощью «цифрового конверта»;  ● при шифровании с помощью асимметричного алгоритма;  ○ посредник необходим всегда, так как он несет юридическую ответственность. |
| Вопрос **11**  Выберите один ответ | Для чего используется алгоритм Диффи-Хеллмана? |
| ○ при шифровании с помощью асимметричного алгоритма;  ● для криптографического протокола, позволяющего двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи;  ○ для нахождения больших взаимно простых чисел и передача их по незащищенному каналу связи;  ○ входит в сертификат открытого ключа. |
| Вопрос **12**  Выберите один или несколько ответов | Что является свойством однонаправленной хэш-функции? |
| ● она необратима;  ○ она монотонна;  ● она имеет конечную область значений;  ○ имеет конечную область определений;  ○ зная хэш-функцию можно получить исходный блок данных. |
| Вопрос **13**  Выберите один ответ | Какой размер результата хэш-функции MD5? |
| ○ 20 байт;  ○ 24 байт;  ● 128 бит;  ○ 256 бит;  ○ 64 байт. |
| Вопрос **14**  Выберите один ответ | На основе какого необратимого преобразования базируется алгоритм RSA? |
| ● Разложения больших чисел на простые множители;  ○ Нахождения корней многочленов *n* степени;  ○ Вычисление логарифма в конечном поле;  ○ Нахождение больших простых и взаимно простых чисел;  ○ Нахождение элементов суммы бесконечного ряда. |
| Вопрос **15**  Выберите один ответ или несколько ответов | В каких алгоритмах количество ключей линейно зависит от количества абонентов в сети? |
| ○ DES;  ○ ГОСТ 12147-89;  ● RSA;  ● Эль-Гамаля. |
| Вопрос **16**  Выберите один ответ или несколько ответов | Какие алгоритмы сжатия относятся к алгоритмам без потерь информации? |
| ○ MP3;  ○ JPG;  ● Хафмана;  ● Лемпеля-Зива. |
| Вопрос **17**  Выберите один ответ или несколько ответов | Какие требования предъявляются к стегосистеме? |
| ● Свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле;  ○ Размер контейнера должен совпадать с размером скрываемой информации;  ● Для повышения надежности встраиваемое сообщение должно быть продублировано;  ○ Встраиваемое сообщение должно быть зашифровано. |
| Вопрос **18**  Выберите один ответ или несколько ответов | На чем основана аутентификация пользователей информационной системы? |
| ● На информации известной только конкретному пользователю.  ○ На информации известной доверенному посреднику;  ● На основании предмета имеющегося у пользователя.  ○ На основании имеющегося сертификата открытого ключа. |