**Тема №2: Информационная безопасность**

***Полужирным выделены правильные варианты ответа на вопрос.***

***Ответы взяты непосредственно из программы после сдачи теста.***

**Вопрос No.1:** Выпишите результат шифрования текста ПРОТОКОЛЫУСТАНОВЛЕНИЯПОДЛИННОСТИ, полученный шифром перестановки с ключом ПРИЕМ. (шифрованный текст получается из столбцов, считываемых сверху вниз в алфавитном порядке следования букв в ключе).

**ТЫННДО\_ОЛАЕОН\_ОУОИЛС\_ПКСВЯИТРОТЛПНИ**

\_ОЛАЕОН\_ОУОИЛС\_ПКСВЯИТРОТЛПНИТЫННДО

ПКСВЯИТРОТЛПНИТЫННДО\_ОЛАЕОН\_ОУОИЛС\_

**Вопрос No.2:** Что из нижеперечисленного может выполнять функцию межсетевого экрана?

**пакетные фильтры**

шлюзы канального уровня

**шлюзы уровня соединения**

**шлюзы уровня приложения**

**Вопрос No.3:** Пусть текст "addds" в английском алфавите шифруется при помощи шифра простой замены. Какова длина ключа?

**26**

33

5

**Вопрос No.4:** К какой атаке уязвим алгоритм Диффи-Хеллмана?

Атака отражением

**Чужой посередине**

Атака подменой

**Вопрос No.5:** Какими свойствами должен обладать электронный аналог ручной подписи?

**Отсутствие возможности получателю подделать документ**

**Отсутствие возможности отправителю позднее отречься от документа**

Должен быть на основе открытого ключа

**Возможность получателю удостовериться в подлинности документа**

**Вопрос No.6:** Какая из схем работы DES является наиболее надежной?

DES с 56-разрядным ключом шифрования

двукратное применение DES с различными ключами K1 и K2

**EDE - схема**

EEE - схема

**Вопрос No.7:** Что из нижеперечисленного относится к недостаткам шлюзов уровня приложений при организации МСЭ?

невысокая стоимость

отсутствие непосредственного сетевого соединения между клиентом и сервером

наличие защиты на уровне приложений позволяет осуществлять большое число дополнительных проверок, снижая тем самым вероятность ее взлома

каждый пакет анализируется вне контекста соединения и сетевого трафика

аутентификация с использованием IP-адреса

ограниченность диапазона параметров фильтрации

**высокая вычислительная сложность**

**низкая производительность**

**Вопрос No.8:** Атака на сеть ЭВМ - это

**действие, заключающееся в поиске и использовании уязвимости сети**

потенциально возможное преднамеренное или непреднамеренное действие, которое может привести к потере безопасности информации

**действие, приводящее к потере безопасности информации**

характеристика сети, которая делает возможным потерю безопасности информации

**Вопрос No.9:** Что является основополагающим фактом надежности алгоритма RSA?

большое количество итераций алгоритма

высокая вычислительная сложность операции взятия квадратного корня

**высокая вычислительная сложность операции разложения на простые множители больших чисел**

секретность алгоритма

**Вопрос No.10:** Выберите два основных принципа шифрования:

**все шифруемые сообщения должны иметь избыточность**

необходимо использовать алгоритмы с секретными ключами

**алгоритм шифрования должен быть открытым**

нужно использовать разные алфавиты для исходного текста и шифрограммы