Тест по модулю «Безопасность информации»

1. Подберите синонимичные прилагательные на русском языке и объясните следующие понятия:

   1) Фейковые новости.

   2) Фейковая программа.

   3) Фейковый номер телефона.

   4) Фейковый аккаунт.

   5) Фейковая страница в социальной сети.

   6) Фейковая кредитная карта.

   7) Фейковый профиль.

   8) Фейковый сайт.

Возможные ответы:

А) Фальшивые новости, ложно смонтированные видео.

Б) Приложение, которые имеет дизайн и функционал, напоминающий переделываемую программу.

В) Виртуальный номер телефона.

Г) Любой аккаунт с недостоверной информацией — имя, контакты, фотографии.

Д) Фиктивная страница в интернет-ресурсах.

Е) Банковская карта, оформленная на человека, который в реальности не существует.

Ж) Профиль, содержащий ложную информацию о владельце либо не содержащую вовсе.

З) Фальсифицированный сайт, копия главной страницы которого напоминает известный.

2. С какими областями деятельности людей чаще всего связаны фейки?

1) Политика.
2) Наука.
3) Реклама и продвижение товаров.
4) Торговля.
5) Обучение.
6) Производство.
7) Маркетинг.
8) Изобретения.
9) Артистическая сфера.
10) Путешествия.

3. Сколько источников и какие именно необходимо просмотреть, чтобы сравнить факты и сделать вывод: является ли эта новость фейковой? Укажите свои источники или выберите из предложенных.

Выберите количество: 1,2,3,4,5

Выберите из предложенных источников:

1) Официальное СМИ.
2) Неофициальное СМИ.
3) Википедия.
4) Интернет-источник.

4. Выберите правильный ответ.

Социальная инженерия – это:

1) Привлечение пользователя к действиям, способствующим заражению вредоносными программами.
2) Метод управления действиями человека без использования технических средств.
3) Технология внедрения вредоносных программ, использующая управление действиями пользователя.

5. Отметьте места, в которых можно безопасно подключиться к общественной сети Wi-Fi?

1) Кафе.
2) Школа.
3) Общественный транспорт.
4) Такси.
5) Ресторан.
6) Торговый центр.
7) Поликлиника.
8) Вуз.

6. Какое шифрование сети, предназначенное для её защиты, легко взломать?

1) WPA.
2) WPA2.
3) WEP.

7. Каковы дополнительные признаки безопасности публичной Wi-Fi сети?

1) Рядом со значком Wi-Fi находится замочек.
2) Для входа в сеть требуется авторизация.
3) Для входа в сеть необходимо ввести пароль.
4) Название сети совпадает с названием учреждения или места расположения.

8. Какие меры безопасности необходимы для проведения онлайн-платежей?

1) Операционная система обновлена.

2) Версия браузера обновлена.

3) Двухфакторная онлайн-транзакция.

4) Компьютер друзей.

5) Свой компьютер.

6) Антивирус, установленный на устройстве, с которого производится транзакция.

7) Обновлённый антивирус, установленный на устройстве, с которого производится транзакция.

8) Правильный адрес в адресной строке.

9) Банковское приложение, скачанное с официального сайта банка.

10) Банковское приложение, скачанное из магазина приложений.

11) Ссылка на страницу из электронного письма или другого источника на онлайн-банкинг.

9. Распределите у себя в тетрадях предложенные действия по столбцам в соответствии с целями необходимости резервного копирования данных.

1) Хранение первоначальной версии операционной системы, не заражённой вредоносными программами.

2) Возможность использования и сохранения последней версии реферата, доклада или других рабочих документов.

3) Защита информации от вредоносного программного обеспечения.

4) Защита от физической порчи флеш-карты.

5) Защита от физической порчи жёсткого диска.

6) Хранение ценных файлов и данных на любом устройстве.

От сбоев оборудования	От случайной потери или искажения хранящейся информации	От несанкционированного доступа к информации

10. Напишите 5 симптомов вероятного заражения вашего устройства вредоносными программами.