НОМИНАЦИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

7 класс

Тестовые задания

Общая часть

Впишите правильный ответ

1. Как называется бытовое оборудование, изображенное на рисунке?

2. Назовите профессии двух сестер – злодеек из «Сказки о царе Салтане» А.С. Пушкина?

3. Предложите три вида промышленных роботов, по характеру выполняемых операций

4. В чем заключается творческий подход к реализации проекта на разных этапах его выполнения: поисково-исследовательском, конструкторско-технологическом и заключительном

Выберите правильный ответ

5. Какой формат является самым маленьким:

а) А0; б) А1; в) А2; г) А3; д) А4

Специальная часть

6. Кража личности подразумевает использование чужих

а) персональных данных

б) документов

в) учётных записей в социальных сетях

г) списков контактов

7. Вводом пароля пользователь системы проходит процедуру

а) авторизации

б) аутентификации

в) запуска пользовательского сеанса

г) проверки прав доступа

8. Верны ли следующие утверждения?

а) Несанкционированный доступ – просмотр информации лицом, не имеющим возможности доступа	Верно	Неверно
б) Среди вредоносных программ различных классов создавать собственные копии могут сетевые черви	Верно	Неверно
в) Основными рисками информационной безопасности являются: искажение, уменьшение объема, перекодировка информации.	Верно	Неверно
г) Когда получен спам по e-mail с приложенным файлом, следует прочитать приложение, если оно не содержит ничего ценного – удалить	Верно	Неверно
д) ЭЦП – это электронно-цифровая подпись	Верно	Неверно

9. В одной IT-компании сотрудники провели усовершенствование систем защиты информации и теперь предоставляют полный цикл услуг по хранению и обеспечению безопасности пользовательских данных в облачном хранилище. Данные мероприятия были проведены из-за того, что недавно системы организации подверглись масштабной атаке, направленной на разные объекты и реализованной различными нарушителями.

Для сбора сведений об информационной системе компании злоумышленники похитили внешний носитель администратора безопасности с паролями нескольких пользователей, при этом больше пароли нигде зафиксированы не были. Реализация этой угрозы нарушила

а) конфиденциальность похищенных данных

б) доступность похищенных данных

в) целостность и доступность похищенных данных

г) конфиденциальность и доступность похищенных данных

д) конфиденциальность и целостность похищенных данных

е) конфиденциальность, целостность и доступность данных

10. Кроме этого, системный администратор немедленно заблокировал учётные записи пользователей, чьи пароли были на похищенном носителе, тем самым

а) повысил защищённость системы компании

б) нарушил доступность информации, к которой имели доступ пользователи

в) остановил утечку информации, к которой имели доступ пользователи

г) нарушил целостность информации в системе компании

д) предотвратил угрозу нарушения конфиденциальности информации на носителе

11. Перед входом в каждый служебный кабинет стоит робот, который получает уведомление о посетителе и просит его пройти аутентификацию, чтобы войти внутрь. Для этого требуется встать на отмеченную позицию перед роботом и замереть на несколько секунд, пока робот проводит «осмотр» и сопоставляет отсканированную картинку с внутренней базой данных сотрудников. Какой тип аутентификации используется?

а) аутентификация по ЭЦП

б) биометрическая аутентификация

в) двухфакторная аутентификация

г) аутентификация на основе фактора знания

д) аутентификация по GPS

12. Не используя пароли с внешнего носителя, нарушители подобрали пароль одного из пользователей, авторизовались в системе под его учётными данными, после чего скопировали его служебные данные и сменили пароль пользователя. Реализация этой угрозы нарушила

а) конфиденциальность данных

б) доступность данных

в) целостность и доступность данных

г) конфиденциальность и целостность данных

д) конфиденциальность и доступность данных

е) конфиденциальность, целостность и доступность данных

13. Вам пришло довольно длинное сообщение с обещанием всяческих благ в случае, если Вы разошлёте это сообщение всем своим друзьям. Какова основная цель подобных рассылок?

а) искреннее желание всем счастья и благ

б) распространение вредоносного ПО

в) получение доступа к персональным данным

г) создание излишней нагрузки на сервер

14. Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, к которым сотрудники должны прикладывать смарт-карты. Какие типы аутентификации реализованы?

а) биометрическая аутентификация

б) аутентификация по ЭЦП

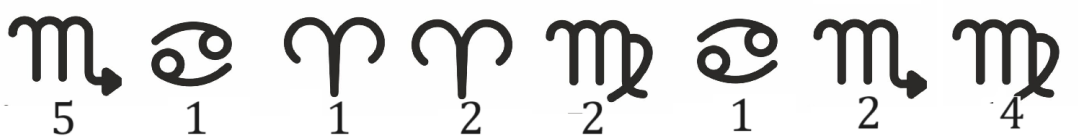
в) однофакторная аутентификация

г) двухфакторная аутентификация

д) многофакторная аутентификация

е) аутентификация на основе фактора владения

15. Однажды мне пришло странное сообщение. Помогите мне его расшифровать.



16. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:

а) контроль доступа
б) аутентификация
в) идентификация
г) тарификация
д) целостность
е) эксплуатация
ж) контроль трафика
з) причастность

17. Системный администратор Трубицын пытается подобрать пароль к компьютеру забывчивого менеджера Петрова. Известно, что Петров не любит придумывать пароли, и пароль представляет собой последовательность из 4 латинских букв, набранных одной рукой в одном ряду клавиатуры, не пропуская клавиш (например, «qwer», «wert», «dfgh» и т. п.). Трубицын набирает пароль почти мгновенно, но компьютер после ввода неправильного пароля делает задержку в 1 минуту. Сколько времени потребуется системному администратору, чтобы подобрать пароль, если правильный вариант пароля — самый последний?

18. Шифр, известный как «квадрат Полибия», устроен следующим образом. В квадратную или прямоугольную таблицу вписываются буквы алфавита (для кодирования – в алфавитном порядке, для шифрования – в произвольном, при этом расположение букв в таблице является ключом), строки и столбцы таблицы обозначаются цифрами. При зашифровании буквы открытого текста заменяются на пары цифр, которыми отмечены, соответственно, строка и столбец, в которых стоит данная буква. Например, на иллюстрации ниже буква «О» зашифрована сочетанием цифр «34», а слово «ОКО» – «34 26 34».

Таким шифром зашифрован некоторый текст (без пробелов, но с сохранением знаков препинания – точки, запятой и вопросительного знака):

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	.	,	?

51 16 32 41 31 34 22 33 16 16 32 16 42 34 15 65 42 16 32 32 16 33 56 52 16 41 13 34 12 34 15 55 64 64

Установите, сколько букв «е» зашифровано в сообщении.

19. Зашифруйте слово «ПОДПИСЬ» по приведённому квадрату Полибия.

Ответ запишите как одно число без разделителей.

20. Напишите пятое слово открытого текста без изменения его написания.

Кейс-задание. (25 баллов)

21. На вокзале города N установлены терминалы самообслуживания. Пассажиру для приобретения билета требуется самостоятельно ввести дату отправления и номер поезда, на который требуется билет, ввести при помощи экранной клавиатуры и встроенного сканера паспортные данные, выбрать место, отсканировать документы, дающие право на приобретение льготного билета, после чего осуществить оплату банковской картой, вставив её в соответствующий разъём терминала и введя PIN-код. Спустя некоторое время

были обнаружены утечки персональных данных пассажиров (паспортных данных и данных других личных документов, сведений о приобретённых билетах) и сведений их банковских карт (номеров карт, сведений о владельцах карт, PIN-кодов и CVV-кодов).

1. Оцените, по каким из физических каналов утечки информации – оптическому, акустическому, радиоэлектронному – нарушители могут перехватить информацию из документов или карты пассажира.
2. Оцените, в какой момент, то есть при совершении пассажиром каких действий, это может произойти.
3. Для каждой определённой Вами возможности перехвата информации

- паспортные данные
- данные прочих документов, дающих право на льготные билеты
- открытую информацию о банковской карте
- CVV-код
- PIN-код

по какому-то конкретному каналу приведите пример того, как (возможно, с помощью каких средств) это может быть совершено. Подтвердите свои оценки и выводы аргументами.

Достаточным является лаконичный ответ, содержащий ответы на пункты 1–3 в сочетании «информация (конкретные данные из приведённых в условии) – канал утечки – момент времени (действия пассажира) – способ реализации угрозы (средство)», например: «Паспортные данные посетителя банка могут быть похищены по оптическому каналу в момент предъявления паспорта охране при помощи скрытой камеры, установленной рядом с постом охраны; телефонный номер может быть похищен по акустическому каналу в момент сообщения его оператору банка при помощи подслушивающего устройства («жучка»), размещённого рядом с рабочим местом оператора».

Рассмотрите все возможные сочетания похищаемой информации и каналов утечки.