Задания по труду (технологии) - ИБ - 7 класс

Общая часть

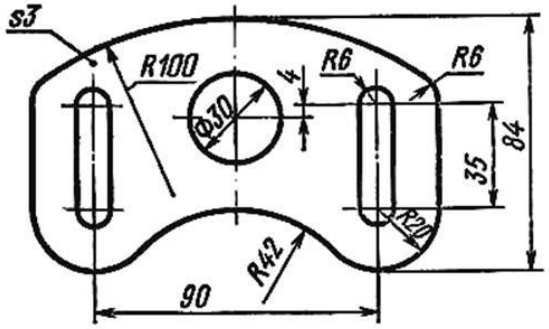
Задание 1. Вставьте пропущенное слово.
Обычно промышленные технологии состоят из нескольких частей, которые называются ___?___ технологиями.

Задание 2. Выделяют три основные составляющие любого интерьера. Одна из них «функциональность и психологическая атмосфера». Перечислите другие две.

Задание 3. Искусственно созданный материал состоящий из нескольких компонентов – это ___?___. Впишите слово (одна ячейка = одна буква).

Задание 4. Начертите электрическую схему, состоящую из проводов, источника тока (гальванического элемента), двух электрических ламп и трех выключателей (ключей). При включении первого ключа должна загораться лампа №1. При включении второго ключа должна загораться лампа №2. При включении третьего ключа должны гореть обе лампы.

Задание 5.



Чертеж выполнен в масштабе **2,5 : 1**. Определите (ответы указывайте в мм):
– А) действительный радиус окружности, изображенной на чертеже в центре детали;
– Б) действительный размер детали по горизонтали (габариты – от левого до правого края детали).

Специальная часть

Задание 6. 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 «М» зашифрована сочетанием цифр «32», а слово «МИР» – «32 24 36».

	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	.	,	?

Таким шифром зашифрован некоторый текст (без пробелов, но с сохранением знаков препинания – точки, запятой и вопросительного знака):
41 32 34 42 36 16 42 56 33 16 31 56 23 63 65 42 34 31 56 26 34 41 31 43 52 11 42 56 64 41 34 13 16 53 11 33 24 63 34 42 32 16 33 16 33 55 64
Установите, сколько точек зашифровано в сообщении.

Задание 7. Напишите предпоследнее слово открытого текста (*смотрите зашифрованное сообщение в задании 6*) без изменения его написания.

Задание 8. По приведённому квадрату Полибия зашифруйте слово «КЛЮЧ». Ответ запишите как одно число без разделителей.

Задание 9. Определите, какое слово зашифровано шифртекстом
36 16 33 34 13 11 46 24 63.
– А) РЕПУТАЦИЯ. – Б) РЕНОВАЦИЯ. – В) РЕПЕТИЦИЯ

Задание 10. Установите шифробозначение (замену) буквы «Г» в шифртексте 35 36 34 44 36 11 32 32 11

Задание 11. Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, при этом руководитель отдела информационной безопасности решил заменить пропуска на универсальный ключ доступа. Какой тип аутентификации тут предусмотрен?
– А) _однофакторная аутентификация_
– Б) _двухфакторная аутентификация_
– В) _многофакторная аутентификация_

Условие (описание ситуации) для заданий №№ 12-15:
В компании «N» усовершенствовали системы защиты информации и теперь предоставляют полный цикл услуг по хранению и обеспечению безопасности пользовательских данных в облачном хранилище. После этого системы организации подверглись атаке, направленной на разные объекты и реализованной различными нарушителями.

Задание 12. Выберите все правильные ответы. 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) _доступность похищенных данных_
– Б) _конфиденциальность похищенных данных_
– В) _целостность похищенных данных_

Задание 13. Обнаружив пропажу, системный администратор немедленно заблокировал учётные записи пользователей, чьи пароли были на похищенном носителе, темсамым
– А) _нарушил доступность информации, к которой имели доступ пользовати_
– Б) _предотвратил угрозу нарушения конфиденциальности информации на носителе_
– В) _нарушил целостность информации в системе компании_

Задание 14. Выберите все правильные ответы. 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) _доступность данных_
– Б) _конфиденциальность данных_
– В) _целостность данных_

Задание 15. Выберите все правильные ответы. Для нанесения финального удара нарушители одновременно провели DDoS- атаку на облачное хранилище компании, а также проникли в него и изменили права доступа одного из клиентов к его базе данных таким образом, чтобы он больше не мог запрашивать из неё сведения. Реализация этой угрозы нарушила
– А) _доступность данных_
– Б) _конфиденциальность данных_
– В) _целостность данных_

Условие (описание ситуации) для заданий №№ 16-19:
В компании «E» усовершенствовали систему информационной безопасности. После этого информационная система компании стала целью атаки со стороны злоумышленников.

Задание 16. Сначала нарушители решили скомпрометировать системы шифрования компании, для чего осуществили перехват ключа шифрования в момент передачи с аппаратного носителя в систему шифрования. Реализация такой угрозы нарушила
– А) _доступность похищенных данных_
– Б) _конфиденциальность похищенных данных_
– В) _целостность похищенных данных_

Задание 17. Выберите все правильные ответы. После успешной компрометации ключа шифрования нарушители перехватили несколько передаваемых по сети зашифрованных сообщений и, заблокировав их

доставку получателю, прочли их и подменили на собственные, которые затем были отправлены по назначению. Реализация такой угрозы нарушила
– А) _доступность похищенных данных_
– Б) _конфиденциальность похищенных данных_
– В) _целостность похищенных данных_

Задание 18. В другом случае нарушители просто исказили хранимую на сервере в зашифрованном виде информацию таким образом, чтобы при попытке её расшифровать пользователь получал лишь бессмысленный набор символов.. Реализация такой угрозы нарушила
– А) _доступность хранимых данных_
– Б) _конфиденциальность хранимых данных_
– В) _целостность хранимых данных_

Задание 19. Помимо системы шифрования целью атаки стала и система электронной подписи, разработанная компанией. Однако ещё до действий нарушителей отправитель (один из сотрудников компании) ошибся в выборе ключа генерации подписи, в результате чего отправленное сообщение не могло пройти проверку подлинности подписи на стороне получателя. Такие действия отправителя
– А) _не нарушили безопасность передаваемой информации_
– Б) _нарушили достоверность передаваемой информации_
– В) _нарушили доступность передаваемой информации_
– Г) _нарушили целостность передаваемой информации_

Условие (описание ситуации) для заданий №№ 20-23:
Компании «М» требуется уделять внимание обеспечению целостности обрабатываемой информации.

Задание 20. Укажите, какую из предложенных ниже мер предпочтительно использовать самой компании для контроля целостности пользовательских данных, хранимых в облачном хранилище. Эти данные могут передаваться и храниться клиентами в зашифрованном виде.
– А) _надежные цифровые водяные знаки_
– Б) _функции хэширования_
– В) _хрупкие цифровые водяные знаки_
– Г) _электронная подпись_

Задание 21. Укажите меру из перечисленных ниже, которая наиболее предпочтительна для клиентов облачного хранилища с целью контроля целостности хранимыхв нём данных.
– А) _надежные цифровые водяные знаки_
– Б) _функции хэширования_
– В) _хрупкие цифровые водяные знаки_
– Г) _электронная подпись_

Задание 22. Передавая партнёрам программные продукты, дальнейшее распространение которых не допускается лицензионным соглашением, компании следует использовать для отслеживания несанкционированного распространения
– А) _надежные цифровые водяные знаки_
– Б) _функции хэширования_
– В) _хрупкие цифровые водяные знаки_
– Г) _электронная подпись_

Задание 23. Укажите две меры, которые компания может использовать для подтверждения внесения клиентами изменений в библиотеки распространённого по лицензиипрограммного обеспечения.
– А) _надежные цифровые водяные знаки_
– Б) _функции хэширования_
– В) _хрупкие цифровые водяные знаки_
– Г) _электронная подпись_

Условие (описание ситуации) для заданий №№ 24-27:
Разработка решений для обеспечения целостности данных – одно из направлений деятельности компании «О».

Задание 24. Одна из наиболее распространённых задач – обеспечение контроля целостности информации, передаваемой по открытым каналам связи. Выберите меру защиты информации, которая подойдёт для решения указанной задачи.
– А) _вычисление контрольной суммы_
– Б) _система хэширования_
– В) _надежные цифровые водяные знаки_
– Г) _электронная подпись_

Задание 25. Одной из категорий продуктов, выпускаемых компанией «О», являются программные средства выработки функций хэширования. Выберите задачу, для решения которой может применяться одно из таких средств.
обеспечение целостности информации, передаваемой по открытым каналам связи
– А) _обеспечение контроля достоверности поступающих сообщений_
– Б) _контроль неизменности отправляемых сообщений_
– В) _обеспечение целостности хранимых на сервере файлов_

Задание 26. Для функций хэширования коллизией называется
– А) _входное значение, для которого не определено выходное значение функции_
– Б) _значение функции, для которого не определено ни одного входного значения_
– В) _пара входных значений, для которых значения функции совпадают_
– Г) _ситуация, когда невозможно корректно вычислить значение функции хэширования_

Задание 27. В отдельных случаях для контроля целостности могут применяться цифровые водяные знаки. Для решения какой задачи они используются?
– А) _контроль неизменности данных, хранимых на сервере_
– Б) _контроль неизменности продуктов, распространяемых по лицензии_
– В) _контроль целостности записей в базе данных_

Условие (описание ситуации) для заданий №№ 28-30:
Руководство банка решило усовершенствовать системы информационной безопасности и для этого внедрить новые способы аутентификации. На основе анализа угроз было принято решение защищать как информационные ресурсы организации, так и служебные помещения от несанкционированного доступа.

Задание 28. Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, к которым сотрудники должны прикладывать смарт-карты. Какие типы аутентификации реализованы? Выберите 2 варианта.
– А) _аутентификация на основе фактора владения_
– Б) _аутентификация по ЭЦП_
– В) _двухфакторная аутентификация_
– Г) _однофакторная аутентификация_

Задание 29. 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 на основе фактора знания
– Б) _аутентификация по ЭЦП
– В) _аутентификация по GPS
– Г) _биометрическая аутентификация

Задание 30. Для запуска компьютера на рабочем месте сотрудника руководство установило следующую систему: сначала она требует ввести PIN-код, после его успешного ввода пользователю требуется поднести электронный ключ к считывателю, а если ключ распознан как корректный, то пользователю предлагается приложить палец к сканеру. Укажите, какая система аутентификации реализована.
– А) _однофакторная аутентификация_
– Б) _двухфакторная аутентификация_
– В) _трёхфакторная аутентификация_

Условие (описание ситуации) для заданий №№ 31-34:
Компания «V» расширила круг предоставляемых услуг и теперь занимается комплексным обеспечением информационной безопасности. К сожалению, недавно одно из её новых решений – система контроля и протоколирования действий пользователей – подверглось атаке злоумышленников с целью демонстрации её слабостей.

Задание 31. Выберите все правильные ответы. На начальном этапе атаки нарушители внедрили в базы данных систем, в которых было развёрнуто решение от компании «V», вредоносную программу, которая могла блокировать или искажать (каждое из этих действий было реализовано примерно в половине заражённых систем) записи о действиях пользователей. Реализация такой угрозы нарушила
– А) _доступность похищенных данных_
– Б) _конфиденциальность похищенных данных_
– В) _целостность похищенных данных_

Задание 32. После реализации описанной выше угрозы часть клиентов отказались от использования системы и самостоятельно удалили или заблокировали собранную информацию об активности собственных сотрудников. Такое действие
– А) _не нарушили информационную безопасность_
– Б) _нарушили доступность удаленных данных_
– В) _нарушили конфиденциальность удаленных данных_
– Г) _нарушили целостность удаленных данных_

Задание 33. Выберите все правильные ответы. Другие клиенты компании «V» приняли решение передать собранные данные на хранение в облачное хранилище, уже контролирующееся нарушителями. Что могут нарушить злоумышленники, полностью контролируя такое хранилище?
– А) _доступность хранимых данных_
– Б) _конфиденциальность хранимых данных_
– В) _целостность хранимых данных_

Задание 34. Стремясь снизить последствия от воздействия на развёрнутые у клиентов продукты, компания приняла решение без ведома клиентов сохранять копии собираемой в их системах информации на своих серверах, передавая её в зашифрованном виде по сети Интернет. Такое действие, относительно информации клиентов
– А) _обеспечило конфиденциальность собираемой информации_
– Б) _нарушило конфиденциальность собираемой информации_
– В) _нарушило доступность собираемой информации_
– Г) _никак не повлияло на информационную безопасность_
– Д) _обеспечило целостность собираемой информации_

Условие (описание ситуации) для заданий №№ 35-38:
Для обеспечения возможности надёжного использования своих продуктов компания «V» принимает меры по обеспечению целостности хранимых записей.

Задание 35. Укажите меру из предложенных ниже, подходящую для контроля целостности записей на сервере, сохраняемых в виде файлов, в которые не производится запись.
– А) _система контроля версий_
– Б) _функции хэширования_
– В) _цифровая подпись_
– Г) _электронная подпись_

Задание 36. Для схем цифровой подписи открытый (публичный) ключ используется для
– А) _вычисления значения функции хэширования_
– Б) _для формирования электронной подписи_
– В) _зашифрования отправляемых сообщений_
– Г) _проверки электронной подписи_

Задание 37. Строя коллизию для известной функции хэширования, нарушитель стремится
– А) _нарушить целостность отправляемого сообщения_
– Б) _не дать возможность заметить внесённые в передаваемую информацию изменения_
– В) _осуществить подмену информации, от которой вычислена функция_
– Г) _подобрать входное значение функции, для которой известен результат вычисления функции_

Задание 38. Для качественной функции хэширования одним из требований является
– А) _отсутствие коллизий, вычисляемых при известной размерности выходного значения_
– Б) _простота вычисления прообраза_
– В) _простота вычисления значения функции_
– Г) _существенное изменение значения функции при внесении изменений во входное значение_

Условие (описание ситуации) для заданий №№ 39-40:
Руководство МФЦ стремится повысить уровень защищённости для своих сотрудников, для чего решило усилить меры аутентификации на ряде позиций объекта.

Задание 39. Для обеспечения пропускного режима в организации была нанята охрана и установлены пропускные турникеты. Сотрудник должен поднести к турникету пропуск, представляющий собой смарт-карту, при этом охранник визуально определяет, соответствует ли входящий фотографии, отображаемой на экране. Какой тип аутентификации реализован?
– А) _двухфакторная на основе факторов знания и владения
– Б) _двухфакторная на основе факторов знания и биометрии
– В) _двухфакторная на основе факторов владения и биометрии

Задание 40. Каждому директору выдаётся служебный ноутбук для работы в корпоративной сети вне офиса. Ноутбук имеет сенсорную панель, клавиатуру, качественный микрофон со встроенной системой распознавания голоса и камеру. Для входа требуется ввести логин и пароль от учётной записи пользователя, с которой связано портативное электронное средство аутентификации, его требуется представить системе (подключить к ноутбуку). Какой тип аутентификации реализован?
– А) _двухфакторная на основе факторов знания и владения_
– Б) _двухфакторная биометрическая на основе факторов знания и владения_
– В) _двухфакторная на основе факторов знания и биометрии_

Рекомендации для выполнения задания № 41:
Достаточным является лаконичный ответ, содержащий ответы на пункты 1–3 в сочетании «информация (конкретные данные из приведённых в условии) – канал утечки – момент времени (действия пилотов или этапы полёта) – 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.

Задание 41. На вокзале 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 соответствующийразъём 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.

Для каждой определённой вами возможности перехвата информации (в т.ч.: а) паспортные данные; б) данные прочих документов, дающих право на льготные билеты; в) открытую информацию о банковской карте; г) CVV-код; д) PIN-код) по какому-то конкретному каналу приведите пример того, как (возможно, с помощью каких средств) это может быть совершено. Подтвердите свои оценкии выводы аргументами