ШИФР_____

профиль «Информационная безопасность»

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ 10-11 КЛАССОВ

Общая часть

1. Выберите верный ответ. (4 балла)

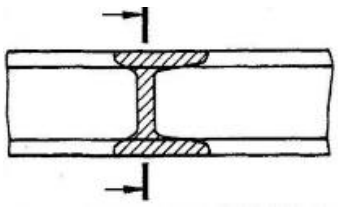
Безотходной технологией называют такой принцип организации производства продукции, который подразумевает ...

1) использование сырья и энергии в замкнутом цикле
2) обезвреживание отходов
3) захоронение отходов
4) сжигание отходов

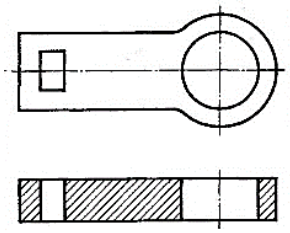
Ответ: _____

2. Выберите правильный ответ(ы). (4 балла)
Определите, где представлены сечения?

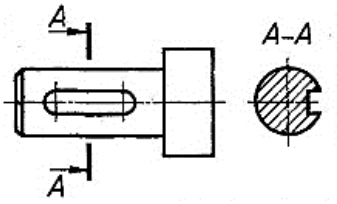
А)

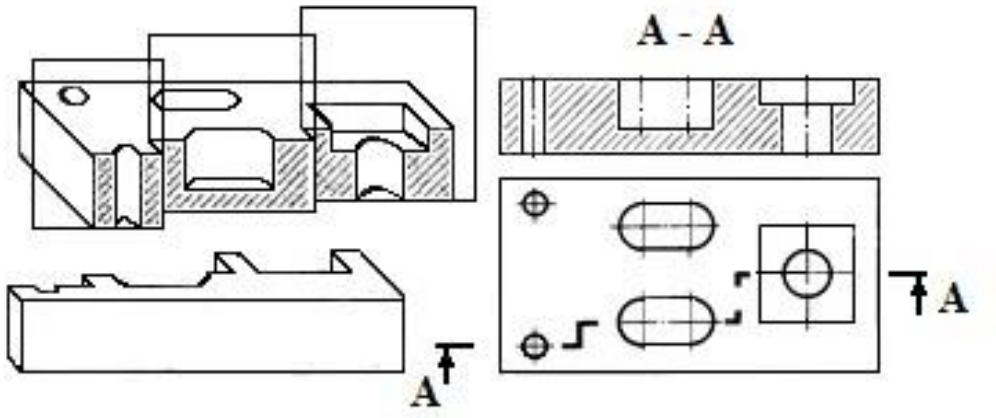


Б)



В)





Ответ: _____

ШИФР_____

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ 10-11 КЛАССОВ

3. Что из перечисленного лучше всего характеризует понятие «стартап»? (4 балла)

а) Малый бизнес, который стремится к росту за счет инноваций
б) Бизнес с многолетней историей
в) Малый бизнес с ограниченным количеством сотрудников
г) Любой новый бизнес, созданный без инвестиций

Ответ: _____

4. Вопрос на соответствие. (4 балла)

Соотнесите предпринимательские термины с их определениями. Поставьте в таблицу соответствующие определениям буквы:

предпринимательские термины	**определения**
1 - Рентабельность	а) Система передачи прав на ведение бизнеса по модели франчайзера.
2 - Инвестиции	б) Вложения капитала в проекты или компании с целью получения прибыли.
3 - Дивиденды	в) Показатель, характеризующий эффективность использования ресурсов для получения прибыли.
4 - Франчайзинг	г) Часть прибыли компании, выплачиваемая акционерам.

Ответ: 1-_____ 2-_____ 3-_____ 4-_____

5. Решите задачу и выберите верный из предложенного перечня вариантов ответов (1 балл):

Магазин электроники продает три товара:
- смартфоны по 30 000 рублей,
- планшеты по 15 000 рублей
- наушники по 5 000 рублей.

В течение дня было продано 10 смартфонов, 15 планшетов и 20 наушников.

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ 10-11 КЛАССОВ

Вопрос: Рассчитайте общую выручку за день и прибыль, если расходы составляют 70% от выручки.

Варианты ответов:

а) Общая выручка: 437 500 рублей; прибыль: 187 500 рублей
б) Общая выручка: 625 000 рублей; прибыль: 187 500 рублей
в) Общая выручка: 187 500 рублей; прибыль: 625 000 рублей
г) Общая выручка: 187 500 рублей; прибыль: 437 500 рублей

Решение:

Ответ: _____

Специальная часть

6. Дан список утверждений. Оцените, является ли верным каждое из них. (3 балла)

Утверждение 1.
«В ОС Windows, от расширения файла зависит, в какой программе он будет открыт по умолчанию»

Утверждение 2.
«Для изображений понятия разрешение и расширение – это синонимы»

Утверждение 3.
«Шифр — совокупность обратимых преобразований множества всевозможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей»

Утверждение 4.
«Цифровая подпись – это фотография или рисунок обычной подписи»

Утверждение 5.
«Файлы cookie – это небольшие фрагменты текста, передаваемые в браузер с сайта, который вы открываете. С их помощью сайт запоминает информацию о ваших посещениях»

Ответ: _____

7. Какие из указанных операционных систем (или их дистрибутивов) не имеют уязвимости информационной безопасности? (3 балла)

1. Microsoft Windows 11
2. Astra Linux 1.7.4
3. Debian 11.8
4. macOS 13.4
5. Android 14
6. Все операционные системы имеют уязвимости информационной безопасности

Ответ: _____

ШИФР_____

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ 10-11 КЛАССОВ

8. 0xAA / 0x5 = ? Укажите все верные варианты. (3 балла)

1. 0xAF
2. 0x96
3. 0x22
4. 0xACDC

Ответ: _____

9. При атаке нарушители внедрили в базы данных систем, вредоносную программу, которая могла блокировать или искажать записи о действиях пользователей. Реализация такой угрозы нарушила: (3 балла)

1. Конфиденциальность данных
2. Доступность данных
3. Целостность и доступность данных
4. Конфиденциальность и доступность данных
5. Конфиденциальность и целостность данных
6. Конфиденциальность, целостность и доступность данных

Ответ: _____

10. http://example.com/view.php?template=admin.php - какая уязвимость? (3 балла)

1. SQLi (SQL Injection)
2. XSS (Cross-Site Scripting)
3. LFI (Local File Inclusion)
4. RFI (Remote File Inclusion)

Ответ: _____

ШИФР_____

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ 10-11 КЛАССОВ

11. Что можно отнести к функциям брандмауэра? Укажите все верные варианты. (3 балла)

1. Анализ сигнатур
2. Фильтрация трафика
3. Защита системы от внешних атак
4. Сканирование на вирусы

Ответ: _____

12. При получении сведений о потенциальной киберугрозе, которая может подвергнуть опасности конфиденциальные данные вашей компании. Какие действия из предложенных следует предпринять, в роли ответственного за информационную безопасность, для обнаружения киберугрозы? (3 балла)

1. Мониторинг сетевой активности и поиск аномалий в поведении систем
2. Сканирование всех компьютеров в сети на наличие вредоносных программ
3. Отключение от интернета всей сети компании для предотвращения утечки данных

Ответ: _____

13. Установите соответствие между угрозой и ее описанием. (6 баллов)

Название	Функции
1. SQL-инъекции	а. Злоумышленник внедряет вредоносный код на веб-страницу, которую затем просматривают другие пользователи.
2. Межсайтовый скриптинг (XSS)	б. Злоумышленник отправляет специально подготовленное обращение от имени пользователя, чтобы выполнить нежелательные действия, такие как изменение пароля или совершение покупки.
3. Межсайтовая подделка запросов (CSRF)	в. Злоумышленник отправляет большое количество запросов на сервер с различных источников.
4. DDoS-атаки	г. Злоумышленники становятся третьим звеном в коммуникации двух людей и перехватывают важные сведения.
5. MITM	д. Злоумышленник вводит вредоносный код в поле ввода, что позволяет ему получить доступ к базе данных сайта.

Ответ: _____

ШИФР_____

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ 10-11 КЛАССОВ

14. В какая модель основана на наборе полномочий, привязанных к конкретным должностям или рабочим задачам? (3 балла)

1. Дискреционной
2. Мандатной
3. Ролевой

Ответ: _____

15. Укажите, верно ли следующее утверждение. (3 балла):

«Бинарная эксплуатация — это категория задач, в которых, как правило, нужно искать и эксплуатировать уязвимости в скомпилированных приложениях»

Ответ: _____

16. Какой маски подсети не существует? (3 балла)

1. 255.255.255.0
2. 128.0.0.0
3. /31
4. 192.000.000.000
5. /64

Ответ: _____

17. Для передачи помехоустойчивых сообщений в алфавите, который содержит 8 различных символов, используется равномерный двоичный код. Этот код удовлетворяет следующему свойству: в любом кодовом слове содержится четное количество единиц (возможно, ни одной). Какую наименьшую длину может иметь кодовое слово? (3 балла)

1. 2 бита
2. 4 бита
3. 5 бит
4. 8 бит

Ответ: _____

18. Имеется следующий запрос:

https://melkomyagkie.com/view.php?template=http://some.site/remote_code.php

Чем является данный запрос и что он может выдать при отсутствии защиты от данной уязвимости и почему? В ответе укажите уязвимость, и обоснование, почему (как) это работает. (7 баллов):

Решение:

19. CVSS (Common Vulnerability Scoring System) — это стандарт оценки уязвимостей в программном или программно-аппаратном комплексе, который позволяет оценить их серьезность и возможное влияние.

Описание уязвимости:

В популярном текстовом редакторе обнаружена уязвимость, связанная с обработкой файлов. Злоумышленник может создать простой вредоносный файл, который, будучи открытым пользователем, запускает произвольный код с правами пользователя. Для эксплуатации уязвимости необходимо, чтобы пользователь сам открыл файл.

Задачи:

1. Определите вектор CVSS 3.1, используя предложенные варианты из таблицы ниже

Вектор CVSS 3.1 записывается следующим образом: сначала записывается версия CVSS «CVSS:3.1», затем пишутся компоненты вектора и его значения (сокращенное обозначение компоненты вектора, двоеточие, сокращенное значение компоненты вектора). Версия и компоненты вектора со значениями отделяются разделителем «/». Порядок перечисления компонент вектора важен. Пример правильной записи:

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/C:L/I:L/A:L`

2. Обоснуйте выбор каждой из компонент вектора

3. Оцените уровень угрозы (является ли уязвимость серьезной) на основе вектора CVSS. Ответ обоснуйте

(10 баллов)

ШИФР_____

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ 10-11 КЛАССОВ

Таблица 1. Компоненты вектора CVSSv3.1 и некоторые его возможные значения

Название компоненты вектора	**Сокращенное обозначение компоненты вектора**	**Возможные значения компоненты вектора**					
		Название значения	**Обозначение**	**Название значения**	**Обозначение**	**Название значения**	**Обозначение**
Attack Vector (Вектор атаки)	AV	Network (через сеть)	N	Local (локально)	L		
Attack Complexity (Сложность атаки)	AC	High (сложно)	H	Low (просто)	L		
Privileges Required (Требование прав доступа)	PR	None (не требуются)	N	Low (требуются)	L		
User Interaction (Взаимодействие пользователя)	UI	None (не требуется)	N	Required (требуется)	R		
Scope (Влияние на другие компоненты системы)	S	Unchanged (не выходит за пределы компонента)	U	Changed (выходит за пределы системы и оказывает влияние на другие компоненты)	C		
Confidentiality (Влияние на конфиденциальность)	C	None (отсутствует)	N	Low (незначительное влияние)	L	High (значительное влияние)	H
Integrity (Влияние на целостность)	I	None (отсутствует)	N	Low (незначительное влияние)	L	High (значительное влияние)	H
Availability (Влияние на доступность)	A	None (отсутствует)	N	Low (незначительное влияние)	L	High (значительное влияние)	H

Ответ:

20. НоноКардано

Решетка Кардано - метод шифрования, где текст записывается через окошки в сетке, которую поворачивают на определенные углы для заполнения всех клеток. Для расшифровки нужно наложить ту же решетку на зашифрованный текст и прочитать его, следуя тем же поворотам.

Нонограмма - логическая головоломка, где игрок закрашивает клетки на сетке, основываясь на числовых подсказках, чтобы создать изображение. Числа указывают количество подряд закрашенных клеток в каждой строке и столбце.

Вы перехватили сообщение, которые было зашифровано с помощью решетки Кардано. Вы не знаете точного расположения отверстий на решетке и угла, но знаете количество подряд вырезанных клеток в каждой строке и каждом столбце.

Также, вы знаете, что решетку надо повернуть и применить дважды (поворот-применение-поворот-применение).

Расшифруйте и запишите исходное сообщение.

(12 баллов)

Перехваченное зашифрованное сообщение:

			3				1	1	1	1		
			5	2	1		1	1	1	1	1	6
			п	н	е	з	а	в	и	ы	я	т
	1	6	д	д	л	с	м	б	о	в	ч	з
	1	1	м	у	л	н	й	а	й	я	а	р
	1	1	а	т	с	с	в	е	о	т	о	м
		1	н	м	л	й	н	ч	у	ь	и	а
	1	1	с	к	м	н	л	ф	т	б	д	с
3	4	1	т	ю	ь	ч	м	о	м	ю	у	у
		2	п	о	а	у	р	ж	о	л	п	а
		1	е	т	з	а	к	а	с	и	п	т
		1	п	л	е	н	ы	и	б	о	г	а

Ответ:

21. Вы работаете в быстро растущей компании и обеспечиваете кибербезопасность, чтобы поддерживать ее доход. Ранее за кибербезопасность отвечала наемная IT-служба, но, теперь, с сегодняшнего дня, была сформирована команда из нескольких человек по техническому обслуживанию и обеспечению информационной безопасности с вами во главе.
Вам необходимо в первый день выбрать первичные действия для обеспечения мер по построению защищенной инфраструктуры корпорации. Вы ограничены в ресурсах. У вас есть ограниченное финансирование в размере 400 тыс. руб. и всего один день - 40ч. Каждое из решений требует вливания финансов и/или времени.

Ваша задача состоит в том, чтобы проанализировать исходное состояние компании и недавние события, а затем выбрать принимаемые решения, исходя из ограниченности ресурсов. Вы не можете превысить расходы (потратить больше 400 тыс. руб.) или исказить время (потратить больше 40ч.).

1. Описание корпорации:
Компания "ТехноЛог": Компания по разработке программного обеспечения. В офисе работают 50 сотрудников, каждый из которых использует настольный компьютер на базе Windows 10. Компания также управляет корпоративным сервером для разработки и тестирования своих продуктов, на котором хранятся критические данные, включая код и конфиденциальную информацию клиентов. Офис имеет две локальные сети: одну для внутренних сотрудников и другую для удалённых клиентов и партнёров, которая предоставляет доступ к продуктам компании для тестирования и обратной связи.

Сотрудники:
- 40 разработчиков
- 5 менеджеров проектов
- 3 специалиста службы поддержки
- 2 IT-специалиста (включая вас)

2. Недавние события:

Событие А: Несколько сотрудников сообщили о подозрительных электронных письмах, в которых содержатся ссылки на неизвестные файлы и подозрительные вложения.

Событие Б: Корпоративная сеть, используемая для работы с клиентами и партнёрами, была скомпрометирована, что привело к утечке данных клиентов.

Событие В: Было обнаружено, что в течение последних двух месяцев не выполнялись резервные копии критических данных с серверов.

Событие Г: Несколько рабочих станций разработчиков показали признаки заражения вредоносным ПО, что привело к замедлению работы и возможному доступу к конфиденциальным данным.

Событие Д: Веб-сайт компании подвергся неудачной попытке взлома, которая, по всей вероятности, была направлена на получение доступа к базе данных клиентов.

3. Перечень ресурсов:

Финансы: 400 тыс. руб.
Время: 40 часов

4. Перечень возможных решений:

Решение	Затраты в финансах (тыс. руб.)	Временные затраты (часов)
1. Тренинг для сотрудников по безопасности, включая распознавание фишинговых писем	50 тыс. руб.	4 ч.
2. Установка системы защиты от фишинговых атак на корпоративную почту	60 тыс. руб.	6 ч.
3. Проведение анализа и устранение последствий утечки данных клиентов	100 тыс. руб.	12 ч.
4. Установка системы мониторинга для отслеживания подозрительных действий в корпоративной сети	40 тыс. руб.	8 ч.
5. Восстановление процедуры регулярного резервного копирования и создание резервной инфраструктуры	0 тыс. руб.	8 ч.
6. Установка нового антивирусного ПО на рабочие станции разработчиков	90 тыс. руб.	6 ч.
7. Проведение анализа рабочих станций разработчиков и устранение заражений	70 тыс. руб.	8 ч.
8. Усиление защиты веб-сайта компании, включая обновление межсетевых экранов и защиту базы данных	110 тыс. руб.	10 ч.
9. Установка системы многофакторной аутентификации для доступа к корпоративной сети	60 тыс. руб.	6 ч.
10. Внедрение системы автоматического резервного копирования данных	30 тыс. руб.	6 ч.

Укажите выбранные решения и обоснуйте выбор каждого из них. Какой вывод можно сделать по поводу процесса выбора принимаемых решений и обеспечению защиты от угроз информационной безопасности?

(12 баллов)

Ответ: