ШИФР_____

профиль «Информационная безопасность»

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ 7-8 КЛАССОВ

Общая часть

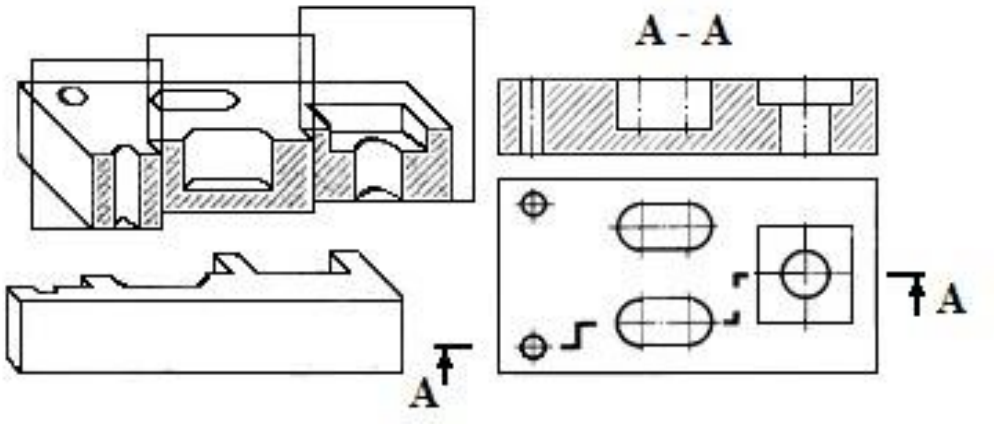
1. Выберите верный ответ. (4 балла)

Технологические знания об использовании и преобразовании материалов, энергии и информации важны в первую очередь

1. при анализе физических явлений
2. при изучении химических процессов
3. при рассмотрении биологических объектов
4. при проектировании и изготовлении изделий

Ответ: _____

2. Назовите вид разреза детали, представленного на чертеже. (4 балла)



Ответ: _____

3. Определите, какой из следующих факторов является ключевым для успешного бизнеса? (4 балла)

а) Высокая цена на товар
б) Хороший маркетинг
в) Низкие расходы на аренду
г) Ограниченное количество сотрудников

Ответ: _____

4. Процесс создания и управления бизнесом предполагает разработку бизнес-плана. Какое из предложенных определений отвечает на вопрос: «Что такое бизнес-план»? (4 балла)

а) Документ с перечнем сотрудников
б) Стратегия ведения бизнеса, описывающая его цели и способы их достижения
в) Отчет о прибыли за год
г) План мероприятий для повышения продаж

Ответ: _____

5. Решите задачу и выберите правильный ответ из перечисленных вариантов. (4 балла)

Вы владеете кофейней.

Ваши расходы на аренду, зарплаты и ингредиенты составляют - 100 000 рублей в месяц.
Средний чек составляет - 200 рублей.
Количество клиентов в день — около 50 человек.

Вопрос: Сколько дней нужно работать в месяц, чтобы кофейня стала прибыльной?

Варианты ответов:

а) более 15 дней
б) более 14 дней
в) более 10 дней
г) 30 дней

Решение:

Ответ: _____

Специальная часть

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

Утверждение 1.
«Информация — сведения (сообщения, данные) независимо от формы их представления»

Утверждение 2.
«MAC-адрес — уникальный идентификатор, присваиваемый каждой единице сетевого оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet»

Утверждение 3.
«Хэширование позволяет преобразовать машинный код (код, который исполняется компьютером) обратно в исходный код»

Утверждение 4.
«Симметричные алгоритмы шифрования используют закрытый и открытый ключ»

Утверждение 5.
«10.123.30.47 — это частный IP-адрес»

Ответ: _____

7. Как еще можно записать маску сети /25? (3 балла)

1. /5 * 5
2. /32
3. 255.255.255.0
4. 255.255.255.128
5. 25.0.0.0
6. 25.25.25.0

Ответ: _____

8. 0xFF = ? Укажите все верные варианты. (3 балла)

1. 255_{10}
2. 256_{10}
3. 11111111_{2}
4. FF_{16}
5. 2024_{10}
6. 1110_{2}

Ответ: _____

9. Модели доступа к данным — это системы распределения полномочий в информационной инфраструктуре компаний. Их ключевая задача — обеспечить необходимый уровень безопасности ресурсов и упростить контроль доступа.

Что из нижеперечисленного является моделями доступа? (3 балла)

1. Дискреционная модель
2. Мандатная модель
3. Ролевая система
4. Разграничение доступа на основе атрибутов
5. Все перечисленное является моделями доступа

Ответ: _____

10. Укажите название атаки, заключающейся в том, что злоумышленнику удается внедрить на страницу JavaScript-код? (3 балла)

1. SQL Injection
2. IP-Spoofing
3. IP-Inclusion
4. XSS

Ответ: _____

11. Какие уровни секретности сведений, составляющих государственную тайну, существуют в Российской Федерации? Укажите все верные варианты. (3 балла)

1. Исключительно секретно
2. Особой важности
3. Совершенно секретно
4. Секретно

Ответ: _____

12. Как называется кибер-атака, в рамках которой мошенник выдаёт себя за какой-либо надёжный источник, чтобы получить доступ к важным данным или информации? (3 балла)

1. Троян
2. Червь
3. Бэкдор
4. Руткит
5. Спуфинг

Ответ: _____

13. Сопоставьте название и функции уровней стека TCP/IP. (6 баллов)

Название	Функции
1. Канальный уровень (Network Access Layer).	а. Регламентирует маршрутизацию, происходящую через запрос на определённый IP-адрес с использованием маски. Для хостов, маркированных одной маской и находящихся в общей подсети, передача данных проходит напрямую.
2. Транспортный уровень (Transport Layer)	б. Решает вопросы поддержки сеансов связи, трансформации данных, взаимодействия с пользователями и сетями.
3. Прикладной уровень (Application Layer)	в. Отвечает за контроль доставки пакетов данных без дублирования и за повторный запрос информации при обнаружении ошибок.
4. Межсетевой уровень (Internet Layer)	г. Поддерживает шифровку данных, разбивку их на пакеты и транспортировку по конкретным каналам. Также в функционал этого уровня входит измерение параметров сигналов, таких, например, как задержка ответов или расстояние между хостами.

Ответ: _____

14. Какого уровня не существует в модели OSI? (3 балла)

1. Сеансового
2. Канального
3. Транспортного
4. Физического
5. Динамического

Ответ: _____

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

«XSS – это уязвимость, при которой злоумышленники создают поддельные сайты, которые выглядят как настоящие, и отправляют жертвам электронные письма или сообщения с просьбой ввести свои данные»

Ответ: _____

16. Сколько IP-адресов доступно внутри сети с маской /16? (3 балла)

1. 255
2. 256
3. 65535
4. 65536
5. 160000

Ответ: _____

17. В компании ООО «Нас не взломают» действует нерушимое правило: все пароли сотрудников уникальны (не может быть двух сотрудников с одинаковым паролем) и должны состоять из 6 символов (количество букв одинаковое во всех паролях). При этом используются только 6 символов: П, А, Р, О, Л и Ь. Какое максимальное количество сотрудников может работать в данной компании при такой политике установки паролей? (3 балла)

Ответ: _____

18. Для кодирования некоторой последовательности, состоящей из букв П, А, Р, О, Л и Ь решили использовать неравномерный двоичный код, позволяющий однозначно декодировать двоичную последовательность, появляющуюся на приёмной стороне канала связи. Для букв П, А, Р, О и Л использовали такие кодовые слова: П–11, А–001, Р–011, О–010, Л-000.

Укажите, каким кодовым словом может быть закодирована буква Ь. Код должен удовлетворять свойству однозначного декодирования. Если можно использовать более одного кодового слова, укажите кратчайшее из них. (7 баллов)

Ответ: _____

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 веб-приложении найдена уязвимость, которая позволяет без особых усилий удалённо выполнить абсолютно любой вредоносный код (RCE) неавторизированному пользователю.

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)

профиль «Информационная безопасность»

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 один раз.

Расшифруйте и запишите исходное сообщение.

(12 баллов)

Перехваченное зашифрованное сообщение:

					8 1	1 1	1 3	1	5	1 1 2	4 3 1	2 1	4 1 3	1 1
			4	5	к	ы	о	м	п	м	ч	я	и	т
			1	3	о	п	р	о	ы	ж	ы	и	в	а
		1	1	1	е	т	ф	а	ч	н	о	н	ы	н
		1	1	1	а	д	н	е	п	о	к	е	п	а
				1	н	й	а	с	ш	а	ч	и	с	п
			1	5	ы	ц	е	в	ы	а	н	ч	б	о
		1	1	1	б	а	ч	е	а	й	о	р	л	ф
1	1	1	1	1	к	о	п	ч	ч	а	в	в	а	д
		1	2	1	р	о	ы	р	а	п	о	а	ч	а
		3	3	2	т	н	ы	е	ш	т	а	н	а	с

Ответ:

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ 7-8 КЛАССОВ

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 100 тыс. руб. и всего один день - 24ч. 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 100 тыс. руб.) или исказить время (потратить больше 24ч.).

1. Описание корпорации:

«Быстрая помощь» - сеть аптек. Сеть из 8 аптек, каждая оснащена двумя кассовыми терминалами и офисным компьютером для менеджера. Все системы работают на базе Windows 10, а данные передаются на центральный сервер в головном офисе. Офис оборудован сервером и двумя ПК.

Сотрудники:

- 24 фармацевта (по 3 на аптеку)
- 8 менеджеров аптек
- 6 сотрудников логистики в центральном офисе
- 4 IT-специалиста (включая Вас)

2. Недавние события:

Событие А. Несколько филиалов сообщили о неоднократных попытках несанкционированного доступа к кассовым терминалам и офисным компьютерам аптек

Событие Б. В системах было обнаружено наличие устаревших антивирусных программ, которые не обновлялись более 6 месяцев

Событие В. Веб-сервер, на котором хранится база данных клиентов и заказов, подвергся подозрительным DDoS-атакам в течение последних 3 дней

3. Перечень ресурсов:

Финансы: 150 тыс. руб.
Время: 24 часа

4. Перечень возможных решений:

Решение	Затраты в финансах (тыс. руб.)	Временные затраты (часов)
1. Тренинг для сотрудников по предотвращению атак на кассы и компьютеры	80 тыс. руб.	6 ч.
2. Установка и настройка нового единого антивирусного ПО на все системы	70 тыс. руб.	6 ч.
3. Проведение ручного анализа всех попыток взлома и настройка систем мониторинга	0 тыс. руб.	12 ч.
4. Установка и настройка системы DDoS-защиты на сервере	100 тыс. руб.	4 ч.
5. Обновление всех систем и программного обеспечения до актуальных версий	0 тыс. руб.	8 ч.
6. Проведение инвентаризации данных, создание системы резервного копирования и резервной системы на случай сбоев	30 тыс. руб	8 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: