

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ИНФОРМАТИКЕ
ПРОФИЛЬ: «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
МУНИЦИПАЛЬНЫЙ ЭТАП
2025/2026 учебный год
9 КЛАССЫ

ТЕОРЕТИЧЕСКИЙ ТУР

Ключи к заданиям

Задание 1. (1 балл). Верный ответ: **е**.

1 балл за верный ответ: **е**; либо: участник перечислил **все** обязательные пункты документа:

а, б, в, г, д.

Обязательные пункты документа о согласии на обработку персональных данных:

- а. Цель обработки персональных данных
- б. Перечень обрабатываемых данных
- в. Срок действия согласия
- г. Порядок отзыва согласия
- д. Подписи сторон

Задание 2. (2 балла) Обязательно должны быть указаны:

- Наименование или ФИО и адрес оператора
- Перечень действий с данными
- Способы обработки данных

Задание 3. (2 балла) Анализ ситуации

Правильные ответы на вопросы:

- а. Нарушения:
 - Публикация информации, позволяющей идентифицировать личность
- б. Возможные последствия:
 - Кража личных данных
 - Мошенничество
 - Преследование
 - Опасность для личной безопасности
- в. Меры предосторожности:
 - Не указывать личную информацию
 - Использовать настройки приватности
 - Не добавлять незнакомцев в друзья
 - Сообщать родителям о подозрительных сообщениях
- г. Куда обращаться:
 - К родителям или законным представителям
 - В администрацию социальной сети
 - В правоохранительные органы
 - В Роскомнадзор при нарушении законодательства

Задание 4. (1 балл) Анализ ситуации

- а. Риски:
 - Потеря денег
 - Кража личных данных
 - Мошенничество
- б. Проверка надёжности:
 - Поиск отзывов
 - Проверка официального сайта
 - Консультация с родителями
- в. Меры предосторожности:
 - Не вкладывать деньги
 - Не сообщать личные данные
 - Обсудить предложение с родителями

Задание 5. (4 балла) Основные шаги по настройке безопасного аккаунта

- Создание пользователя
- Назначение группы
- Установка пароля
- Настройка прав доступа
- Ограничение доступа к системным файлам

Задание 6. (4 балла) Ограничение доступа пользователей к системным командам.

- а. Инструменты для ограничения доступа:
 - /etc/sudoers
 - SELinux/AppArmor
 - Группы пользователей
- б. Настройка списка команд:
 - Редактирование файла sudoers
 - Создание алиасов команд
 - Ограничение доступа через shell
- в. Возможные риски:
 - Потеря доступа к системе
 - Нарушение работоспособности приложений
 - Уязвимости безопасности
- г. Проверка настроек:
 - Тестирование доступа от имени пользователя
 - Проверка логов аудита
 - Использование команд id, groups, sudo -l

Задание 7. (3 балла) Описать процесс передачи файла.

- файл разбивается на пакеты (обычно 1500 байт);
- каждый пакет получает IP-заголовок с адресами отправителя и получателя;
- маршрутизаторы определяют оптимальный путь для каждого пакета;
- протокол TCP обеспечивает надёжность передачи;
- на компьютере Б пакеты собираются в исходном порядке.

Задание 8. (3 балла) Проблемы с маршрутизацией.

- а. Факторы влияния:
 - Загруженность каналов связи
 - Правильность построения маршрутов
 - Нагрузка на маршрутизаторы
 - Конфигурация сетевых устройств
- б. Протоколы для оптимизации:
 - RIP (Routing Information Protocol)
 - OSPF (Open Shortest Path First)
 - BGP (Border Gateway Protocol)
- в. Проверка настройки:
 - Команда ping
 - Команда traceroute
 - Проверка таблиц маршрутизации
- г. Инструменты мониторинга:
 - Утилита netstat
 - Программа Wireshark
 - Системные журналы (логи)

Задание 9. (2 балла) Зашифрованная фраза «дай списать задание по информатике.»
Пробелы в шифре опущены.

Задание 10. (4 балла) Варианты усложнения шифра:

- изменить порядок символов алфавита;
- изменить нумерацию ячеек (использовать трёхзначные/шестнадцатеричные числа)
- использовать матрицу переменного размера (размер матрицы становится частью ключа, периодически менять матрицу в процессе шифрования). Вариант — использование нескольких матриц с разным порядком следования символов и периодической сменой их в процессе шифрования;
- двойное шифрование (например, сначала изменить порядок букв с помощью шифра со сдвигом, потом зашифровать по матрице);
- динамическое перемещение символов (например, базовая матрица заполняется по алфавиту, выбирается ключ-число, через определенное количество символов происходит сдвиг символов, правила сдвига определяются ключом).

Задание 11. (5 баллов) Шифр Виженера, ключевое слово — пятница, ответ
НАЧИНАТЬВСЕГДАСТОИТСОГОЧТОСЕЕТСОМНЕНИЯ ИЛИ
НАЧИНАТЬ ВСЕГДА СТОИТ С ТОГО, ЧТО СЕЕТ СОМНЕНИЯ

Задание 12. (5 баллов) Анализ фрагмента трафика

- DNS (порт 53)
- отправитель: 192.164.1.100, получатель: 77.88.8.8 (Яндекс DNS)
- это DNS-запросы
- порт 53 — стандартный порт DNS-сервера, а отправитель использует эфемерные порты

Задание 13. (4 балла) Название атаки «Перехват DNS-запросов». Атака заключается в замене ответов настоящего DNS-сервера на вредоносные IP-адреса.

Когда вы вводите адрес в поисковую строку, веб-браузер ищет информацию о веб-странице в кэше локальной памяти (если вы ранее уже посещали эту страницу) или отправляет DNS-запрос на сервер системы доменных имен (обычно предоставленный интернет-провайдером). Процесс обмена данными между браузером и сервером системы доменных имен наиболее уязвим для атаки, поскольку данные передаются в незашифрованном виде. Именно в этот момент злоумышленники перехватывают запрос и подменяют ответ. Киберпреступники используют четыре различных способа перехвата DNS-запроса: локально, на уровне роутера, на уровне DNS-сервера и по типу man-in-the-middle («человек посередине»).

Задание 14. (4 балла) Запись 10.12.74.22/29 — IP адрес.

- его сетевая маска $255.255.255.248 = 29$
- адрес сети 10.12.74.16/29
- широковещательный адрес 10.12.74.23
- всего хостов в сети 6
- доступные адреса хостов от 10.12.74.17 до 10.12.74.22

Задание 15. (5 баллов) Данная запись является командами настройки брандмауэра ufw.

`ufw allow 3000:3100/tcp` — разрешает входящий TCP-трафик через диапазон портов от 3000 до 3100 включительно

`ufw deny 3000:3100/udp` — запрещает входящий UDP-трафик через тот же диапазон портов (3000-3100)

Т.е. эти две команды создают следующую конфигурацию:

- любой TCP-трафик в диапазоне портов 3000-3100 будет пропущен через файрвол;
- любой UDP-трафик в этом же диапазоне портов будет заблокирован.

Такая конфигурация может быть использована для сервисов, которые:

- используют TCP для нормальной работы;
- не должны использовать UDP в этом диапазоне портов (для безопасности);
- хотят предотвратить возможные атаки через UDP-протокол.

Задание 16. (5 баллов) Данная запись является командами настройки брандмауэра iptables

`iptables -A INPUT -s 11.22.121.0/24 -j REJECT` — добавляет правило в цепочку INPUT (входящий трафик). В результате все входящие пакеты из подсети 11.22.121.0/24 будут отклонены, и отправитель получит уведомление о том, что его пакеты не приняты.

`iptables -A OUTPUT -d 31.13.78.35 -j DROP` - добавляет правило в цепочку OUTPUT (исходящий трафик). В результате все исходящие пакеты, направленные на IP-адрес 31.13.78.35, будут удалены системой без уведомления отправителя.

Задание 17. (4 балла) Фрагмент трафика

- а. попытка передачи HTTP-трафика (порт 80) на HTTPS-порт (443) может указывать на атаку;
- б. проверить источник трафика, заблокировать подозрительный IP.

Задание 18. (6 баллов)

`iptables -A INPUT -p tcp --dport ssh -s 10.10.10.10 -j DROP`

или

`ufw deny from 10.10.10.10 to any port 22`

Задание 19. (2 балла) В Римской империи для доставки сообщения выбирали раба, голову которого брили, а затем с помощью татуировки наносили текст. После того, как волосы отрастали, раба отправляли адресату. Получатель сообщения снова обривал голову раба и читал сообщение.

Этот метод сокрытия информации называется «стеганография» (от греч. *στεγανός* — скрытый + *γράφω* — пишу; буквально «тайнопись») — технология, позволяющая спрятать передаваемые данные в некотором контейнере, скрыв сам факт передачи информации.

Задание 20. (4 балла) Фишинговое письмо.

- а. Сомнения в достоверности.
- б. Это фишинговое письмо.
- в. Письмо от органа власти, но приветствие в письме обезличенное, заголовок вызывает тревогу, в подписи к письму отсутствуют контактные данные. Приведённый код, будучи размещённым на сайте, позволит злоумышленникам получить к нему доступ.