

Задания и критерии проверки для проведения муниципального этапа ВсОШ по информатике (профиль «Информационная безопасность») в 2025-2026 у.г.

7-8 классы

Раздел 1: Теоретические задания (Основы безопасности) (3балла)

Задание 1. Базовые понятия.

Что из перечисленного является наибольшей угрозой конфиденциальности данных?

- а) Вирус-шифровальщик (Ransomware)
- б) Сетевой сканер портов
- в) Фишинговая атака, направленная на кражу логинов и паролей
- г) DDoS-атака на веб-сайт

Ответ: в) Фишинговая атака, направленная на кражу логинов и паролей, так как она напрямую ведет к утере контроля над конфиденциальной информацией.

Задание 2. Парольная политика.

Петя создает пароль для своего почтового ящика. Какой из предложенных паролей является наиболее стойким и почему? Ответ обоснуйте.

- а) `qwerty12345`
- б) `ПетяИванов2007`
- в) `J8\$qL2!nPm`
- г) `1234567890`

Ответ: в) `J8\$qL2!nPm`. Он содержит буквы в разном регистре, цифры и специальные символы, не является словарным словом или предсказуемой последовательностью.

Задание 3. Защита от вредоносного ПО.

Что такое "антивирус с проактивной защитой" (эвристический анализ)?

- а) Лечение уже зараженных файлов.
- б) Обновление вирусных баз данных.
- в) Анализ поведения программ и выявление подозрительных действий, даже если вирус еще не известен.
- г) Проверка только входящей почты.

Ответ: в) Анализ поведения программ и выявление подозрительных действий.

Раздел 2: Практические задания (Поиск уязвимостей и логика) (3 балла)

Задание 4. Шифрование (Цезарь).

Вам перехватили зашифрованное сообщение: `ПЬОМПЯБГЧЙ`. Известно, что использовался русский алфавит и шифр Цезаря со сдвигом. После расшифровки вы получили осмысленное слово. Какое это слово?

Подсказка: Сдвиг постоянный, пробуйте разные варианты.

Ответ: `КОМПЬЮТЕР` (сдвиг на -1, или +32).

Задание 5. "Кто взломал аккаунт?".

Аккаунт Маши был взломан. Под подозрением трое ее друзей: Алексей, Борис и Виктор. Известно, что взломал только один.

- * Маша сказала: "Это сделал Алексей".
- * Алексей сказал: "Это сделал Виктор".
- * Борис сказал: "Алексей лжет".
- * Виктор сказал: "Это сделал не я".

Известно, что двое говорят правду, а двое лгут. Кто взломал аккаунт?

Ответ: Виктор. (Правду говорят Борис и Виктор, лгут Маша и Алексей).

Задание 6. Поиск фишинговой ссылки.

Вам пришло письмо от "службы поддержки Facebook" с просьбой срочно проверить настройки безопасности. В письме есть ссылка: `https://faceb00k-security.secure-login.com`. Объясните, почему эту ссылку можно считать фишинговой (укажите не менее двух причин).

Ответ:

1. Доменное имя второго уровня (SLD) — `faceb00k-security`, а не `facebook`. Буквы 'o' заменены на zeros '0', чтобы обмануть пользователя.
2. Настоящий домен Facebook — `facebook.com`, а здесь используется поддомен `secure-login.com`.

Раздел 3: Прикладные и ситуационные задания (4 балла)

Задание 7. Безопасное соединение.

Как пользователь может визуально убедиться, что его соединение с сайтом банка защищено и передаваемые данные шифруются?

Ответ: Необходимо проверить два элемента в адресной строке браузера:

1. Наличие `https://` в начале адреса (а не `http://`).
2. Наличие значка закрытого замка.

Задание 8. Двухфакторная аутентификация (2FA).

Объясните, что такое двухфакторная аутентификация, и приведите пример из повседневной жизни (не связанный с компьютерами).

Ответ: Это метод защиты, при котором для доступа требуется предоставить два разных типа доказательств (фактора). Пример: снятие денег в банкомате (1-й фактор: банковская карта, 2-й фактор: ПИН-код).

Задание 9. Общественный Wi-Fi.

Почему безопаснее не вводить пароли от социальных сетей и банковских аккаунтов, подключившись к открытому публичному Wi-Fi в кафе?

Ответ: Трафик в открытых сетях часто не шифруется, и злоумышленник, находящийся в той же сети, может "прослушать" (перехватить) ваши данные.

Задание 10. Юридический аспект.

С какого возраста, согласно Федеральному закону РФ "О персональных данных", можно давать согласие на обработку своих персональных данных?

- а) С 14 лет
- б) С 16 лет
- в) С 18 лет

г) С 6 лет

Ответ: б) С 16 лет (согласно ст. 9 ФЗ-152, с некоторыми оговорками).

Раздел 4: Задания повышенной сложности (4 балла)

Задание 11. Стеганография.

Стеганография — это...

- а) Наука о шифровании данных.
- б) Наука о сокрытии самого факта передачи сообщения.
- в) Наука о создании секретных чернил.
- г) Наука о кодировании информации.

Ответ: б) Наука о сокрытии самого факта передачи сообщения (например, скрывание текста внутри изображения).

Задание 12. Логика и права доступа.

В файловой системе есть три типа прав: Чтение (R), Запись (W), Выполнение (X). Владелец файла установил для себя права `rwx`, для своей группы — `r-x`, а для всех остальных — `r--`. Может ли пользователь, не входящий в группу владельца, изменить (отредактировать) этот файл?

Ответ: Нет. Права для "всех остальных" — только на чтение (`r--`), права на запись (`w`) отсутствуют.

Задание 13. Безопасность IoT (Интернета вещей).

Почему умная лампочка или детская Wi-Fi-игрушка могут представлять угрозу безопасности домашней сети?

Ответ: Такие устройства часто имеют слабые стандартные пароли, устаревшее и необновляемое программное обеспечение с уязвимостями. Взломав такую "вещь", злоумышленник может получить точку входа в домашнюю сеть.

Задание 14. Этичный хакер.

Кто такой "этичный хакер" (white hat hacker) и чем он занимается?

Ответ: Это специалист по кибербезопасности, который ищет уязвимости в системах и программном обеспечении с разрешения их владельца, чтобы помочь устранить эти уязвимости до того, как ими воспользуются злоумышленники.

Практические задания 7-8 класс. (25 баллов)

Задание 1: «Расшифруй послание» (Криптография) (5 баллов)

Условие:

Вам перехватили зашифрованное сообщение, которое было отправлено агенту. Известно, что использовался шифр Цезаря с постоянным сдвигом для русского алфавита (считаем, что используются только 33 буквы, «ё» нет).

Зашифрованный текст:

`УГЧХВУФКУМАЧЬФХВУФКУМ`

Задание:

1. Расшифруйте сообщение.
2. Определите ключ (сдвиг), который использовался для шифрования.

Критерии оценки:

- * Правильно определенный сдвиг: 2 балла
- * Правильно расшифрованный текст: 3 балла

Задание 2: «Найди злоумышленника» (Логика и аудит) (5 баллов)

Условие:

В небольшой компании произошла утечка данных. Системный администратор предоставил логи входа в защищенную систему за последний час. Известно, что у каждого сотрудника только один аккаунт, и утечка произошла в результате несанкционированного доступа.

Время входа	Имя пользователя	IP-адрес	Успешность
10:05	ivanov	192.168.1.5	Успешно
10:15	petrova	192.168.1.7	Неудачно
10:16	petrova	192.168.1.7	Успешно
10:30	sidorov	192.168.1.8	Успешно
10:45	ivanov	192.168.1.5	Успешно
10:50	petrova	172.16.0.3	Успешно

Задание:

Какую запись в логах вы считаете наиболее подозрительной и почему? Дайте развернутый ответ, указав не менее двух причин.

Критерии оценки:

- * Правильное определение подозрительной записи: 1 балл
- * Объяснение первой причины (например, смена IP): 2 балла
- * Объяснение второй причины (например, подбор пароля): 2 балла

Задание 3: «Собери безопасный пароль» (Парольная политика) (5 баллов)

Условие:

Вам необходимо создать новый пароль для школьного электронного дневника. Требования системы:

- * Длина не менее 8 символов.
- * Обязательно должны присутствовать заглавные и строчные латинские буквы, цифры и один специальный символ из набора: `! @ # \$ % & \*`.

Исходные данные:

Вам пришла в голову фраза: «Мой кот любит спать 10 часов».

Задание:

Преобразуйте эту фразу в стойкий пароль, используя технику основанную на мнемонике (например, взять первые буквы слов или преобразовать слова). Запишите получившийся пароль и кратко опишите использованный алгоритм преобразования.

Пример плохого преобразования: `Mkls10ch` – этот пароль слишком короткий и не содержит специальных символов.

Критерии оценки:

- * Пароль соответствует всем техническим требованиям: 2 балла
- * Пароль не является очевидным и устойчив к угадыванию: 2 балла
- * Дан логичный алгоритм его создания: 1 балл

Задание 4: «Определи фишинг» (Анализ веб-страницы) (6 баллов)

Условие:

Изучите изображение (имитацию) входящего email-письма от имени «Службы безопасности ВКонтакте».

Тема: Срочно! Ваша страница будет заблокирована!

Здравствуйте!

В нашей системе зафиксирована подозрительная активность с вашей страницей. Для предотвращения блокировки необходимо срочно подтвердить ваши данные.

Перейдите по ссылке и войдите в свою учетную запись:

<https://vk-security.com/confirm-page?user=12345>

Если вы не сделаете это в течение 24 часов, доступ к странице будет ограничен.

С уважением, Служба безопасности ВКонтакте.

Задание:

Найдите и перечислите не менее трех признаков, которые указывают на то, что это фишинговое письмо.

Критерии оценки:

- * За каждый верно указанный и аргументированный признак: 1 балл (всего 3 балла)
- * За четвертый и любой последующий верный признак: +1 балл (дополнительно, максимум +2 балла)

Задание 5: «Настрой права доступа» (Управление доступом) (9 баллов)

Условие:

В операционной системе Linux права доступа к файлу задаются для трех категорий пользователей: Владелец (u), Группа (g), Все остальные (o). Права бывают трех типов: Чтение (r=4), Запись (w=2), Выполнение (x=1).

Файл с отчетом `otchet.txt` имеет следующие права: `rw-r--r--`.

Задание:

1. Расшифруйте, что означают текущие права `rw-r--r--` для Владельца, Группы и Всех остальных.
2. Руководство решило, что файл `otchet.txt` должен быть доступен для чтения только владельцу и членам его группы. Все остальные пользователи не должны иметь к нему никакого доступа. Запишите команду на языке Linux, которая установит такие права.

Критерии оценки:

- * Правильная расшифровка текущих прав: 2 балла (по 0.5-1 баллу за каждую категорию)
- * Правильно записанная команда: 3 балла

Ответы и критерии для проверки

Задание 1:

- * Ответ: Сдвиг = 21 (или +21, или -5). Расшифрованное сообщение: `СОВРЕМЕННЫЕ ТЕХНОЛОГИИ`.
- * Критерии: Сдвиг — 2 балла, Текст — 3 балла.

Задание 2:

- * Ответ: Наиболее подозрительна запись `petrova` с IP-адреса `172.16.0.3` в 10:50.
- * Причины:
 1. IP-адрес `172.16.0.3` принадлежит другой подсети, отличной от обычной рабочей (`192.168.1.x`). Это может означать вход извне или с другого устройства.
 2. За 35 минут до этого с аккаунтом `petrova` уже была попытка входа с рабочего IP, которая сначала была неудачной, что может указывать на подбор пароля, после которого злоумышленник смог войти с другого места.
- * Критерии: Запись — 1 балл, каждая причина — по 2 балла.

Задание 3:

- * Пример ответа: Пароль: `MkL\*s10h!`
- * Алгоритм: Взял первые буквы каждого слова фразы, сохранил регистр для существительных. Цифру `10` оставил как есть. Заменял слово «любит» на символ `\*`, а в конец добавил восклицательный знак для соответствия требованиям.
- * Критерии: Соответствие требованиям — 2 балла, Устойчивость — 2 балла, Алгоритм — 1 балл.

Задание 4:

- * Возможные признаки:
 1. URL-адрес: Настоящий домен ВКонтакте — `vk.com`. Ссылка ведет на подозрительный домен `vk-security.com`.
 2. Создание паники: Использование слов «Срочно!», «будет заблокирована» — классический прием, чтобы пользователь действовал не думая.
 3. Требование входа по ссылке: Настоящая служба безопасности никогда не просит переходить по ссылке и вводить логин/пароль в письме.
 4. Ошибки/безличное обращение: «Ваша страница», без указания имени и фамилии пользователя.
- * Критерии: По 1 баллу за каждый из первых трех признаков. Дополнительные баллы за четвертый и пятый.

Задание 5:

- * Ответ:
 1. `gw-g--g--` означает:
 - * Владелец (u): чтение (r) и запись (w).
 - * Группа (g): только чтение (r).
 - * Все остальные (o): только чтение (r).
 2. Команда: `chmod 640 otchet.txt`
- * Критерии: Расшифровка — 2 балла, Команда — 3 балла.