Критерии проверки заданий для проведения муниципального этапа ВсОШ по информатике (модуль «Информационная безопасность»)

для 9-11 класса

2025-2026 уг

Время выполнения заданий 180 минут

Задание 1. Криптография: Шифр Виженера (15 баллов)

Вам перехватили зашифрованное сообщение: «ЦЦВЮЩЬТ ЫДФЖЦЧ». Известно, что оно зашифровано шифром Виженера с ключевым словом «ШИФР». Русский алфавит (33 буквы, от А до Я, без Ё). Задание:

1) Расшифруйте сообщение.
2) Объясните, чем шифр Виженера безопаснее шифра Цезаря.

Ответ: 1) «ИНФОРМАЦИЯ БЕЗОПАСНА», 2) Использование ключевого слова устраняет уязвимость частотного анализа, присущую моноалфавитным шифрам.

Критерии оценивания	***баллы***
Правильный ответ на вопрос 1	10
Правильный ответ на вопрос 2	5
Правильный ответ на 1 и 2 вопросы	15

Задание 2. Сетевая безопасность: Анализ трафика (10 баллов)

Вам дан упрощенный фрагмент сетевого заголовка:

IP-адрес отправителя: 192.168.1.15

IP-адрес получателя: 10.0.2.20

Порт отправителя: 55321

Порт получателя: 23

Ответьте на вопросы:

1) при помощи какой утилиты командной строки можно проверить, доступен ли хост 10.0.2.20?
2) К какому протоколу прикладного уровня относится этот трафик? Является ли этот протокол безопасным для передачи паролей? Ответ обоснуйте.

Ответ:

1) ping
2) Протокол Telnet (порт 23). Не является безопасным, т.к. передает данные, включая пароли, в открытом виде

Критерии оценивания	*баллы*
Правильный ответ на вопрос 1	2
Правильный ответ на вопрос 2	8
Правильный ответ на 1 и 2 вопросы	10

Задание 3. Социальная инженерия: Анализ фишингового письма (10 баллов)

Задача:
Проанализируйте текст электронного письма и найдите не менее 4 признаков, указывающих на то, что это фишинг.

Тема: Срочно! Ваш аккаунт ВКонтакте будет заблокирован!
От: support@vknotakte.ru
Здравствуйте! В нашей системе зафиксирована подозрительная активность вашего аккаунта. Для проверки безопасности перейдите по ссылке и подтвердите ваши данные: `http://vk-security.ru/confirm?user=12345`
С уважением, Служба поддержки ВКонтакте.

Ответ: *Примеры признаков: опечатка в адресе отправителя (vknotakte), подозрительный домен в ссылке (vk-security.ru), создание искусственной срочности, запрос личных данных по ссылке из письма.*

Критерии оценивания	*баллы*
За каждый верно указанный признак	2,5
Максимальный балл	10

Задание 4. Правовая база: Задачи (10 баллов)

Ответьте на вопросы, связанные с законодательством РФ в сфере ИБ.

1) Какой федеральный закон является основным для регулирования отношений в области защиты информации и информационных технологий?
2) С какого возраста в РФ наступает уголовная ответственность за распространение вредоносных компьютерных программ?

Ответы:

Правильный ответ на вопрос 1: Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Правильный ответ на вопрос 2: С 16 лет, по ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Критерии оценивания	*баллы*
Правильный ответ на вопрос 1	5
Правильный ответ на вопрос 2	5
Правильный ответ на 1 и 2 вопросы	10

Задание 5. Практическое задание: Командная строка Windows (10 баллов)
Вам необходимо провести первичный анализ системы на предмет подозрительной активности.

Вопросы:

1) Какой командой можно вывести список *всех* установленных сетевых подключений с отображением PID (идентификатора процесса)?
2) Какой командой можно найти все файлы с расширением .txt в каталоге C:\Scan и его подкаталогах?

Ответ:

Правильный ответ на вопрос 1: netstat -ano.

Правильный ответ на вопрос 2: dir C:\Scan*.txt /s.

Критерии оценивания	***баллы***
Правильный ответ на вопрос 1	5
Правильный ответ на вопрос 2	5
Правильный ответ на 1 и 2 вопросы	10

Задание 6. Защита персональных данных (10 баллов)

Школа собирается внедрить систему пропусков с использованием отпечатков пальцев учеников. Являются ли биометрические данные (отпечатки пальцев) персональными данными согласно законодательства РФ? Назовите не менее двух специальных требований по обработке биометрических данных.

Ответ: Да, являются. *Примеры: необходимость письменного согласия субъекта ПД, необходимость обезличивания, повышенные требования к безопасности хранилищ, запрет на трансграничную передачу без согласия.*

Критерии оценивания	***баллы***
Правильный ответ на первую часть	2
Правильный ответ за каждое верно указанное требование	4
Максимально возможный балл	10

Задание 7. Анализ рисков (10 баллов)

Сотрудник малого бизнеса использует один и тот же простой пароль для почты, облачного хранилища и учетной записи в социальной сети.

Опишите сценарий кибератаки, который может произойти в этой ситуации, и назовите два метода защиты, которые могли бы предотвратить инцидент.

Ответы:

Описание сценария: утечка пароля из соцсети -> злоумышленник проверяет этот пароль на почте -> получает доступ -> через почту инициирует сброс пароля в облаке -> получает доступ к бизнес-документам

Методы защиты: Использование менеджера паролей, включение двухфакторной аутентификации

Критерии оценивания	*баллы*
Описание сценария	5
Правильный ответ за каждый верный метод защиты	2,5
Максимально возможный балл	10

Задание 8. Веб-безопасность: SQL-инъекция (10 баллов)

Дан URL адрес сайта: **http://example.com/news.php?id=15**

Ответьте на вопрос:

1) Какой символ часто используется для проверки уязвимости к SQL-инъекции в таком параметре?
2) Какая основная мера защиты от данной уязвимости?

Критерии:

Правильный ответ на вопрос 1: 5 баллов (Одиночная кавычка `'`).

Правильный ответ на вопрос 2: 5 баллов (Использование подготовленных выражений (prepared statements) или параметризованных запросов).

Задание 9. Криптография: Хэши (5 баллов)

Вам нужно проверить целостность скачанного файла setup.exe. У вас есть эталонный хэш, предоставленный разработчиком: a1b2c3d4e5f67890.

Какой встроенной утилитой командной строки Windows вы можете вычислить *хэш-сумму* файла, чтобы сравнить ее с эталонной?

Правильный ответ: (certutil-hashfile setup.exe MD5 или certutil-hashfile setup.exe SHA256, в зависимости от длины эталонного хэша).

Критерий: 5 баллов

Задание 10. Этика и профессиональная деятельность (10 баллов)

Студент, увлекающийся информационной безопасностью, обнаружил уязвимость в сайте местной администрации, позволяющую получить доступ к данным граждан.

Опишите этически и юридически корректный порядок его действий. Почему нельзя сразу публиковать информацию об уязвимости?

Ответ:

Корректный порядок действий: Фиксация доказательств -> составление ответственного отчета -> отправка отчета администрации сайта/техническому персоналу -> выждать время на исправление

Объяснение: Публикация до исправления предоставляет злоумышленникам инструкцию для атаки и может привести к утечке данных, что является нарушением закона

Критерии оценивания	***баллы***
Корректный порядок действий	7
Объяснение	3
Максимально возможный балл	10