

**МАТЕРИАЛЫ ДЛЯ ЧЛЕНОВ ЖЮРИ  
(КЛЮЧИ, КРИТЕРИИ)  
МАКСИМАЛЬНОЕ КОЛИЧЕСТВО БАЛЛОВ - 60.**

**Общая часть (5 баллов)**

Номер вопроса	Макс балл	Правильный ответ
<b>Общая часть</b>		
1	1	5
2	1	2,1,3
3	1	13158
4	1	1-В, 2-А, 3-Г, 4-Б, 5-Е, 6-Д
5	1	2175

**Специальная часть (45 баллов)**

1	2	Федеральное Агентство Правительственной Связи и Информации Комплексная система защиты информации
2	2	ПРИНЦИПАМИ
3	5	Верно: 1,2,4. Неверно: 3,5
4	2	1
5	2	2
6	2	3
7	2	3
8	2	2
9	2	2
10	4	1,3
11	6	1-Б,В,Е 2-А,Г,Д
12	5	Ключ сдвига: 5 (1 балл) Расшифрованный текст: Стеганография, криптография-отличные способы сохранить пароль в секрете. Для базы данных я применяю пароль слово гарантия. (по 0,25 балла за слово)
13	9	Везде исследуйте всечасно, Что есть велико и прекрасно. (по 1 баллу за слово, по 0,25 баллов за знак препинания)

**Кейс-задание (10 баллов)**

Какие действия могли предпринять работники NASA, чтобы выявить причину заражения и как обезвредить? Укажите два основных действия с обоснованием (**5 баллов, по 2,5 балла за каждое действие с обоснованием**).

С какими угрозами информационной безопасности можно столкнуться в наши дни и как с ними бороться? Укажите две основные угрозы и обоснуйте их выбор (**5 баллов, по 2,5 балла за каждое действие с обоснованием**).

**Примерные варианты ответов:**

1. Какие действия могли предпринять работника NASA, чтобы выявить причину заражения и как обезвредить?

Причины заражения:

\*Для быстрого и своевременного выявления причины необходимо было обратиться незамедлительно в Центр национальной компьютерной безопасности США.

\*Чтобы выявить причину заражения нужно просканировать систему антивирусом или антивирусным сканером

\*Антивирусная система СНК4ВОМВ позволяла проанализировать текст загрузочного модуля и выявлять все текстовые сообщения и «подозрительные» участки кода.

Действия:

\*Единственным способом остановить червя было полное отключение компьютера от сети.

\*Буквально за два дня были определены и заблокированы «лазейки», через которые червь проникал в систему, а код заразы был целиком дизассемблирован. За 12 часов активной работы и изучения кода программисты смогли написать закрывающую дыры заплатку и начать распространять её по сети.

\*Вредоносную активность сразу же обнаружили администраторы сети. Они привлекли большое количество разработчиков для борьбы с ней. Решением проблемы занимались специалисты Центра национальной компьютерной безопасности, Национального института науки и технологий, Агентства военной связи, Министерства энергетики США, ЦРУ, ФБР и других организаций США.

2. С какими угрозами информационной безопасности можно столкнуться в наши дни и как с ними бороться?

Угрозы информационной безопасности:

\*Вирусы, черви и трояны — вредоносные программы, которые проникают в компьютер или сеть и наносят различный вред. С их помощью киберпреступники крадут, портят и уничтожают данные.

\*Перехват паролей — процесс получения доступа к чужому аккаунту путем кражи учетных данных.

\*Фишинг — мошенническая практика, когда киберпреступники выдают себя за надежные источники для получения личной информации. Одна из разновидностей фишинга — использование подменных доменных имен, которые похожи на настоящие.

\*Социальная инженерия — манипуляции людьми с целью получения личной информации или выполнения определенных действий. Например, злоумышленник может различными способами втираться в доверие к жертве, ведя с ней переписку в социальных сетях или мессенджерах.

Методы борьбы:

\* Антивирусное и антишпионское ПО. Предназначено для обнаружения и удаления вредоносных программ, таких как вирусы, трояны, шпионские программы.

\*Криптография. Обязательно шифруйте данные, это играет важнейшую роль в их защите. Шифрование информации при передаче и хранении помогает предотвратить утечки, причем даже при компрометации системы в целом. Это процесс преобразования исходных данных в зашифрованные с помощью специального алгоритма, который называют ключом. Таким образом, криптографическая защита делает информацию непонятной для всех, кто таким ключом не владеет.

\*Управление доступом. Разграничьте права и используйте дополнительную защиту. Речь прежде всего о программных ограничениях доступа — разграничении пользователей при помощи аутентификации с различными правами.

\*Программная защита. Установите дополнительное ПО. Программная защита включает использование антивирусов и антишпионских программ, брандмауэров (межсетевых экранов) и других средств для обнаружения и предотвращения киберугроз. Такие программы защитят корпоративную сеть от вирусов, червей, троянов, руткитов, кейлоггеров, шпионского и рекламного ПО (adware), программ-вымогателей. А брандмауэры снижают риск несанкционированного доступа и DDoS-атак.

\*VPN и прокси. VPN (виртуальные частные сети) и прокси-серверы обеспечивают безопасное соединение с сетью через шифрование трафика, что позволяет защитить информацию при передаче через открытые сети.

\*Сканеры уязвимостей. Используются для поиска уязвимостей в сетях, приложениях и устройствах, чтобы предотвратить возможные кибератаки.