

**ВСЕРОССИЙСКАЯ ОЛИМПИАДА ПО ТЕХНОЛОГИИ.
МУНИЦИПАЛЬНЫЙ ЭТАП
Теоретический тур
номинация
«Информационная безопасность»
возрастная группа 10-11 класс**

Уважаемое жюри!

Вам предстоит оценить теоретические задания участников олимпиады.

Задание теоретического тура считается выполненным, если участник вовремя сдаете его членам жюри.

Максимальная оценка – 100 баллов.

Номер задания	Баллы	Комментарии
1	2	2 балла за полный ответ, в остальных случаях – 0 баллов
2	2	2 балла за полный ответ, в остальных случаях – 0 баллов
3	2	2 балла за полный ответ, в остальных случаях – 0 баллов
4	2	2 балла за полный ответ, в остальных случаях – 0 баллов
5	2	2 балла за полный ответ, в остальных случаях – 0 баллов
6	6	2 балла за каждое совпадение
7	1	1 балл за полный ответ, в остальных случаях – 0 баллов
8	2	1 балла за 3 верных ответа, 2 балла за полный ответ
9	3	3 балла за полный ответ, в остальных случаях – 0 баллов
10	1	1 балл за полный ответ, в остальных случаях – 0 баллов
11	1	1 балл за полный ответ, в остальных случаях – 0 баллов
12	1	1 балл за полный ответ, в остальных случаях – 0 баллов
13	2	1 балла за 2 верных ответа, 2 балла за полный ответ
14	1	1 балл за полный ответ, в остальных случаях – 0 баллов
15	2	2 балла за полный ответ, в остальных случаях – 0 баллов
16	6	2 балла за каждое совпадение
17	3	3 балла за полный ответ, в остальных случаях – 0 баллов
18	10	3 балла за правильный ответ, 7 баллов за верное рассуждение и решение, 10 баллов за полный ответ
19	11	3 балла за правильный ответ, 7 баллов за верное рассуждение и решение, 10 баллов за полный ответ
20	15	10 баллов ответ, 5 баллов решение или рассуждение
21	25	2 балла за каждую правильно выбранную угрозу, 7 баллов за определения
	100	

ОТВЕТЫ ТЕОРЕТИЧЕСКОГО ТУРА

1. a
2. c
3. d
4. Двухфакторная аутентификация
5. a c

6.

1	2	3
c	a	b

7. Нет
8. a b c e f h

9.

1	Ошибки пользователя
2	Ошибки профессионалов
3	Отказы и сбои аппаратуры
4	Форс-мажорные обстоятельства

10. Луркинг
11. шифротекст
12. руткиты
13. a, c, d, f
14. скрытый канал утечки информации
15. a

16.

1	2	3
b, c	a, e	d, f

17. c

18. ответ: 28614

в алфавите горда 7 букв

пароли 6 буквы

*	*	*	*	*	*
ao	альПОНТ	альПОНТ	альПОНТ	альПОНТ	альПОНТ
2	7	7	7	7	7

$2*7*7*7*7*7*7=33614$ различных паролей

$33614-5000=28614$

28614 туристов может пройти в город с уникальным паролем

19. ответ: Учение в счастье украшает, а при несчастье – утешает.

Аня и Катя переписываются с помощью шифра «Код Цезаря», в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. В данном случае на 2 буквы вперед

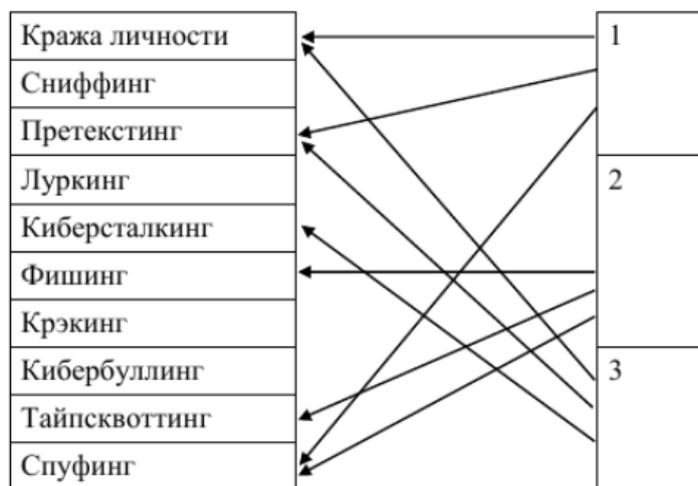
а	б	в	г	д	е	ё	ж	з	и	й
к	л	м	н	о	п	р	с	т	у	ф
х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

20. ответ: Я желаю тебе больших успехов в учёбе

фраза: Желаю не стоять на месте, а смело двигаться вперёд — к новым знаниям, к новым открытиям, к новым мечтам. Желаю тебе больших успехов в учёбе. Желаю никогда не терять энтузиазма. Желаю каждый день встречать с вдохновением и невероятным желанием узнавать что-то новое и важное!

В фразе повторяющиеся буквы заменяются цифрами или редко используемыми буквами

21.



Кража личности — преступление, при котором незаконно используются персональные данные человека для получения материальной выгоды.

Претекстинг — атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию узнает конфиденциальную информацию.

Киберсталкинг — один из видов кибербуллинга, то есть проявления насилия в цифровом пространстве. Киберсталкинг может проявляться в отправке сообщений с угрозами, публикации частной информации без согласия её владельца, целевых хакерских атаках, создании ложных профилей в социальных сетях и на сайтах знакомств, слежке и постоянном комментировании действий жертвы в интернете.

Фишинг — это обман пользователя с целью получения его личных данных, таких как логин, пароль, номер телефона или банковской карты.

Тайпсквоттинг – это вид атак социальной инженерии, нацеленный на пользователей интернета, допустивших опечатку при вводе веб-адреса в браузере и не использующих поисковую систему.

Спуфинг - кибер-атака, в рамках которой мошенник выдает себя за какой-либо надежный источник, чтобы получить доступ к важным данным или информации.