

Пермский край
2023-2024 учебный год
**ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ПО ТЕХНОЛОГИИ
МУНИЦИПАЛЬНЫЙ ЭТАП
10-11 КЛАСС
ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
ТЕОРЕТИЧЕСКИЙ ТУР
КЛЮЧИ**

- 1. А
- 2. С
- 3. С
- 4. 630
- 5. D
- 6. А, В, D

Обоснование:

Солдатова Г. У., Чигарькова С. В., Пермякова И.Д. «Кибербезопасность» учебник для 7 класса общеобразовательных организаций.

Методическое пособие к учебнику Г. У. Солдатовой, С. В. Чигарьковой, И.Д. Пермяковой «Кибербезопасность» для 7 класса общеобразовательных организаций / авт.-сост. Г. У. Солдатова, С. В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022.

Вангородский, С. Н. Основы кибербезопасности : учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019.

- 7. А, С, D

Обоснование:

Солдатова Г. У., Чигарькова С. В., Пермякова И.Д. «Кибербезопасность» учебник для 7 класса общеобразовательных организаций.

Методическое пособие к учебнику Г. У. Солдатовой, С. В. Чигарьковой, И.Д. Пермяковой «Кибербезопасность» для 7 класса общеобразовательных организаций / авт.-сост. Г. У. Солдатова, С. В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022.

Вангородский, С. Н. Основы кибербезопасности : учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019.

- 8. 1) – D; 2) – E; 3) – B; 4) – A; 5) – C

Обоснование:

Солдатова Г. У., Чигарькова С. В., Пермякова И.Д. «Кибербезопасность» учебник для 7 класса общеобразовательных организаций.

Методическое пособие к учебнику Г. У. Солдатовой, С. В. Чигарьковой, И.Д. Пермяковой «Кибербезопасность» для 7 класса общеобразовательных организаций / авт.-сост. Г. У. Солдатова, С. В. Чигарькова, И.Д. Пермякова. — М.: ООО «Русское слово — учебник», 2022.

Вангородский, С. Н. Основы кибербезопасности : учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019.

9. А

10. D

Обоснование:

Федеральный закон «Об информации, информационных технологиях и о защите информации», статья 16. Защита информации

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

11. 1) – F, K, L, M; 2) – C, D, H; 3) – A, B, E, J

Обоснование:

Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". Доктрина информационной безопасности российской федерации.

III. Основные информационные угрозы и состояние информационной безопасности

IV. Стратегические цели и основные направления обеспечения информационной безопасности

В документе предполагается, что ущерб наносится законным правам, свободам или интересам тех или иных субъектов. Не названы конкретные субъекты или объекты, но указываются: личность, общество, государство.

В формулировке ответов указаны конкретные лица и организации, чьим интересам может быть нанесен ущерб. При ответе необходимо учесть, что, например отечественные СМИ, общественные организации, судьи, чья репутация неотделима от репутации государства, Россия как государство, - это не материальные объекты.

По объектам критической информационной инфраструктуры:

V. Организационные основы обеспечения информационной безопасности

33. Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности,

организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

12. В

В соответствии с ФЗ о персональных данных обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. Александр такого согласия Егору не давал («с удивлением обнаружил»).

Статья 6. Условия обработки персональных данных.

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

13. С

Решение:

- определить L: подсчитать количество символов в каждом пароле (колонка «Пароль»);
- определить A: подсчитать количество символов, входящих в пароль (колонка «Символы, входящие в пароль»);
- привести в минуты максимальный срок действия пароля (колонка «Т»);
- рассчитать P для каждого пароля, по указанной формуле, подставив значения V, T, A, L;
- определить из полученных P наименьшее значение (наименьшая вероятность подбора пароля с указанной скоростью перебора паролей (V), с учетом срок а действия пароля (T)). Пароль с этим значением обладает большей стойкостью к атакам перебора (пароль 7^z0gK\$E0R).

Пароль	L	Возможные символы в пароле		V (мин)	T (дней)	T (мин)	P
9%aA8#zZ	8	цифры 0...9; специальные символы: #, %, \$; латинские символы:A, a, Z,z.	16	10	3 дня	4320	1,53477E-10

1\$а8#6b 82сI9#k K6	16	цифры 0...9; специальные символы: #, %, \$, ^; латинские символы: a,b,c,d, I,j,K,k .	20	10	2 дня	2880	2,38228E-20
7^z0gK\$ EOR	10	цифры 0,7; специальные символы: #: #, %, \$, ^; латинские символы: a,A,b,B,d,D,e,E,g,G,z, Z,e,E,g,G,I,i,J,j,K,k,f, F,R,r	32	10	5 дней	7200	7,2E-28
Z3g\$F5 G%D	9	цифры 3,5; специальные символы: #, %, \$, ^; латинские символы: a,A,b,B,d,D,e,E,g,G,z, Z,e,E,g,G,I,i,J,j,K,k,f, F,R,r	32	10	7 дней	1008 0	2,93562E-26
5A3GZ1 E4z%g	11	цифры 1,2,3,4,5; специальные символы: #, %, ^; латинские символы: A,g,G,z,Z,E	14	10	4 дня	5760	1,51679E-10

14. «желаем всем удачи!»

Буквы были пронумерованы

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
желаем всем удачи!

Затем, согласно номерам, вписаны в квадрат

16 !	3 л	2 е	13 а
5 е	10 м	11 у	8 с
9 е	6 м	7 в	12 д
4 а	15 и	14 ч	1 ж

Выписывая друг за другом, получаем строку

!леаемусемвдаичж

15. «Ключ пряник»

Нужно выписать каждую первую букву в словах

Коля любил **ю**жную **ча**сть **па**лисадника, **ра**дуясь **я**рким **на**рциссам **и** **ко**локольчикам

16. 5

Так как $X_2 = 3 * 6 + 1 \pmod{7}$ (или, это остаток от деления 19 на 7), то $X_2 = 5$

17. 2

Очевидно, что поврежденные биты в байтах со значениями 254 и 253. Если перевести их значения в двоичную систему счисления, для 254 получится 1111 1110, для 253 соответственно 111 1101.

18. С

Так как здесь имеем дело с повреждением информации, то возникает проблема с ее целостностью

19. Проблема в том, что при шифровании простой заменой, одинаковые исходные элементы преобразуются в другие, но одинаковые элементы.

Так, если бы мы побайтно шифровали фрагмент картинки

255 255 255 254 255 255 253 255 255

то могли бы получить, например

100 100 100 300 100 100 170 100 100

Здесь просто бы поменялись цвета пикселей.

20. А

Так как здесь имеем дело с желанием владельца зашифровать (ограничить доступ к информации), то нужно решить проблему конфиденциальностью информации.

21.

Решение:

1. Ответ – 155

(правильный ответ – 1 балл, ответ принимается, когда написано 155)

Решение:

$$T_1 = 255 = 11111111_2$$

$$VI = 100 = 01100100_2$$

$$T_1 \oplus VI = 10011011_2 = 155$$

2. Ответ – 55

(правильный ответ – 1 балл, ответ принимается, когда написано 55)

Решение:

$$2 * 155 + 1 = 311$$

Остаток от деления 311 на 256 это 55

3. Ответ – 145

(правильный ответ – 1 балл, ответ принимается, когда написано 145)

Решение:

$$T_2 = 255 = 11111111_2$$

$$C_1 = 55 = 00110111_2$$

$$T_2 \oplus C_1 = 01001000_2 = 72$$

$$2 * 72 + 1 = 145$$

4. Формула расшифрования – $T_1 = D_{a,b}(C_1) \oplus VI$ или $T_1 = VI \oplus D_{a,b}(C_1)$

(правильный ответ – 2 балла, ответ принимается, когда приведена формула

$D_{a,b}(C_1) \oplus VI$ или $VI \oplus D_{a,b}(C_1)$)

Обоснование:

$$\text{Так как } C_1 = E_{a,b}(T_1 \oplus VI),$$

$$\text{то } T_1 \oplus VI = D_{a,b}(C_1)$$

если к $T_1 \oplus VI$ применить еще XOR с VI, т.е. $T_1 \oplus VI \oplus VI$, то получим просто T_1

КРИТЕРИИ ОЦЕНИВАНИЯ

№	Ответы	Баллы
1.	А	1
2.	С	1
3.	С	1
4.	630	1
5.	Д	1
6.	Могут быть написаны пункты ответа А, В, Д или представлены развернутые ответы, соответствующие этим пунктам.	1
7.	Могут быть написаны пункты ответа А, С, Д или представлены развернутые ответы, соответствующие этим пунктам.	1
8.	Должно быть представлено точное соответствие цифр и выбранных пунктов, возможна альтернативная запись, из которой понятны выбранные соответствия 1) – Д; 2) – Е; 3) – В; 4) – А; 5) – С любое несоответствие ведет к потере балла за этот вопрос.	1
9.	Может быть написан пункт ответа А или представлен развернутый ответ, соответствующий этому пункту.	1
10.	Может быть написан пункт ответа Д или представлен развернутый ответ, соответствующий этому пункту.	1
11.	Должно быть представлено точное соответствие цифр и выбранных пунктов, возможна альтернативная запись, из которой понятны выбранные соответствия 1) – F, K, L, M; 2) – C, D, H; 3) – A, B, E, J любое несоответствие ведет к потере балла за этот вопрос.	1
12.	Может быть написан пункт ответа В или представлен развернутый ответ, соответствующий этому пункту.	1

13.	Может быть написан пункт ответа С или представлен развернутый ответ, соответствующий этому пункту.	1
14.	Должна быть написана строка «желаем всем удачи!», она может быть написана без пробелов, так как этот символ не учитывался при шифровании	1
15.	Должна быть написана строка «Ключ пряник».	1
16.	5 Ответ должен быть только 5	1
17.	2 Ответ должен быть только 2	1
18.	Может быть написан пункт ответа С или представлен развернутый ответ, соответствующий этому пункту.	1
19.	В ответе должна быть отражена суть проблемы « при шифровании простой заменой, одинаковые исходные элементы преобразуются в другие, но одинаковые элементы »	1
20.	Может быть написан пункт ответа А или представлен развернутый ответ, соответствующий этому пункту.	1
21.	<i>Оценивается в соответствии с выше данными решениями и комментариями</i>	5
	ВСЕГО БАЛЛОВ	25