ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ИНФОРМАТИКА. ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
2026 г. ПРИГЛАСИТЕЛЬНЫЙ ЭТАП. 4–5 КЛАССЫ

Максимальный балл за работу – 20.

1. Шифр простой перестановки – это шифр, при котором исходный текст делится на блоки определённой длины и буквы в пределах одного блока меняются местами по определённому правилу. Например, при шифровании слова «ПОЧТАЛЬОН», используя блоки длины 3 и перестановку «312», получим следующее:

ПОЧТАЛЬОН ⟶ ПОЧ ТАЛ ЬОН ⟶ ЧПО ЛТА НЬО ⟶ ЧПОЛТАНЬО

Зашифруйте фразу АМЫВЫИГРАЛИОЛИМПИАДУ, разделив предварительно текст на блоки длины 5 и используя перестановку «53142».

Ответ запишите без пробелов.

2. Хакерская группировка атакует правительственные сайты. Для того, чтобы раскрыть её, необходимо решить задачу технического характера.

Есть информация о численности группировки и навыках, которыми владеет каждый хакер. При запросе в базе данных для обозначения логической операции «И» используется символ «&», а для логической операции «ИЛИ» символ «|». В таблице приведены запросы и количество найденных по ним записей.

Запрос	**Найдено**
Социальная инженерия	852
Технические навыки	524
Социальная инженерия | технические навыки	1198

Разумеется, самыми опасными являются те, кто владеют и социальной инженерией, и техническими навыками. Вычислите их количество.

3. Записан набор символов, в котором скрыто осмысленное слово на русском языке:

?_ _ _ **** · _

Также известно, какие символы и комбинации символов соответствуют некоторым буквам русского алфавита.

_ _	* * #	. _	_ _ _	_ !	?	.	*	# .	#	* * *	_	? _
А	Б	Д	Е	З	М	Н	О	Р	С	Т	Х	Ы

- Какое слово скрыто?
- Сколько букв в скрытом слове?

4. Придумайте пароль в соответствии со следующей маской: G_*?.0fK

В маске звёздочка (*) обозначает латинскую букву или цифру. Вопросительный знак же показывает, что на этом месте находится цифра.

Какие **два** из нижеперечисленных паролей соответствуют предложенной маске?

- G_*8.0fK
- G_m4.0fK
- G_*75fK
- G_15.0fK
- J_x?.0fK
- Gk6.0fK

5. Реализацию угроз информационной безопасности можно разделить на этапы.

1. Разведка – нарушитель собирает информацию о потенциальной жертве.
2. Первоначальный доступ – нарушитель, у которого нет прав доступа в систему жертвы, осуществляет проникновение в неё.
3. Закрепление – нарушитель создаёт условия для повторного доступа. Например, меняет права доступа, пароль взломанной учётной записи и т. п.
4. Вывод данных – нарушитель передаёт из взломанной системы похищенные данные.
5. Сокрытие атаки – нарушитель предпринимает меры маскировки своих действий от защитных мер потенциальной жертвы.
6. Вредоносное воздействие – нарушитель реализует цель атаки: похищает, модифицирует, удаляет информацию, выводит из строя или нарушает работы информационной системы и т. п.

Для каждого события выберите соответствующий номер этапа реализации угроз.

	1	**2**	**3**	**4**	**5**	**6**
Случайное повреждение электриком сервера компании						
Удаление базы данных вредоносной программой						
Передача троянской программой похищенных паролей своему владельцу						
Изучение хакером страницы сотрудника компании в социальной сети						
Взлом пароля учётной записи одноклассника в социальной сети						
Создание новой учётной записи администратора во взломанной системе						

Максимальный балл за работу – 20.

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ИНФОРМАТИКА. ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
2026 г. ПРИГЛАСИТЕЛЬНЫЙ ЭТАП. 4–5 КЛАССЫ

ОТВЕТЫ И КРИТЕРИИ ОЦЕНИВАНИЯ

Максимальный балл за работу – 20.

1. Шифр простой перестановки – это шифр, при котором исходный текст делится на блоки определённой длины и буквы в пределах одного блока меняются местами по определённому правилу. Например, при шифровании слова «ПОЧТАЛЬОН», используя блоки длины 3 и перестановку «312», получим следующее:

ПОЧТАЛЬОН ⟶ ПОЧ ТАЛ ЬОН ⟶ ЧПО ЛТА НЬО ⟶ ЧПОЛТАНЬО

Зашифруйте фразу АМЫВЫИГРАЛИОЛИМПИАДУ, разделив предварительно текст на блоки длины 5 и используя перестановку «53142».

Ответ запишите без пробелов.

Ответ: ЫЫАВМЛРИАГМЛИИОУАПДИ

За полностью верный ответ – 3 балла.

2. Хакерская группировка атакует правительственные сайты. Для того, чтобы раскрыть её, необходимо решить задачу технического характера.

Есть информация о численности группировки и навыках, которыми владеет каждый хакер. При запросе в базе данных для обозначения логической операции «И» используется символ «&», а для логической операции «ИЛИ» символ «|». В таблице приведены запросы и количество найденных по ним записей.

Запрос	**Найдено**
Социальная инженерия	852
Технические навыки	524
Социальная инженерия | технические навыки	1198

Разумеется, самыми опасными являются те, кто владеют и социальной инженерией, и техническими навыками. Вычислите их количество.

Ответ: 178

За верный ответ – 3 балла.

3. Записан набор символов, в котором скрыто осмысленное слово на русском языке:

? _ _ _ **** . _

Также известно, какие символы и комбинации символов соответствуют некоторым буквам русского алфавита.

_ _	* * #	. _	_ _ _	_ !	?	.	*	# .	#	* * *	_	? _
А	Б	Д	Е	З	М	Н	О	Р	С	Т	Х	Ы

- Какое слово скрыто?

Ответ: МЕТОД.

За верный ответ – 2 балла.

- Сколько букв в скрытом слове?

Ответ: 5.

За верный ответ – 2 балла.

Максимум за задание – 4 балла.

4. Придумайте пароль в соответствии со следующей маской: G_*?.0fK

В маске звёздочка (*) обозначает латинскую букву или цифру. Вопросительный знак же показывает, что на этом месте находится цифра.

Какие **два** из нижеперечисленных паролей соответствуют предложенной маске?

- G_*8.0fK
- **G_m4.0fK**
- G_*75fK
- **G_15.0fK**
- J_x?.0fK
- Gk6.0fK

За каждый верный ответ – 2 балла.

Если участник указал более 2 ответов, в том числе и правильные – **0 баллов**.
Максимум за задание – 4 балла.

5. Реализацию угроз информационной безопасности можно разделить на этапы.

1. Разведка – нарушитель собирает информацию о потенциальной жертве.
2. Первоначальный доступ – нарушитель, у которого нет прав доступа в систему жертвы, осуществляет проникновение в неё.
3. Закрепление – нарушитель создаёт условия для повторного доступа. Например, меняет права доступа, пароль взломанной учётной записи и т. п.
4. Вывод данных – нарушитель передаёт из взломанной системы похищенные данные.
5. Сокрытие атаки – нарушитель предпринимает меры маскировки своих действий от защитных мер потенциальной жертвы.
6. Вредоносное воздействие – нарушитель реализует цель атаки: похищает, модифицирует, удаляет информацию, выводит из строя или нарушает работы информационной системы и т. п.

Для каждого события выберите соответствующий номер этапа реализации угроз.

	1	**2**	**3**	**4**	**5**	**6**
Случайное повреждение электриком сервера компании						+
Удаление базы данных вредоносной программой						+
Передача троянской программой похищенных паролей своему владельцу				+		
Изучение хакером страницы сотрудника компании в социальной сети	+					
Взлом пароля учётной записи одноклассника в социальной сети		+				
Создание новой учётной записи администратора во взломанной системе			+			

За каждый верный ответ – 1 балл. Максимум за задание – 6 баллов.

Максимальный балл за работу – 20.