ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ 2022/23 гг.
МУНИЦИПАЛЬНЫЙ ЭТАП
ТЕХНОЛОГИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
7-8 КЛАСС

Шифр _____

Задания для обучающихся

ТЕОРЕТИЧЕСКИЙ ТУР

Продолжительность выполнения заданий теоретического тура – 90 минут

Максимальное количество баллов - 65

МОДУЛЬ 1

Тестовые задания (20 баллов)

Матрица ответов на тестовые задания

Номер теста	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Верный ответ										

Номер теста	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Верный ответ										

№ п/п	Тестовые задания	
	Определите один правильный ответ	
1	*Какие вирусы активизируются в самом начале работы с операционной системой:* а. загрузочные вирусы б. троянцы в. черви г. полиформы	1
	Определите один правильный ответ	
2	*Методы установки пароля на документ MS Word:* а. Office - Подготовить - Зашифровать документ б. Главная - Вставка - Пароль в. Office -Главная - Зашифровать документ г. Файл - Сведения - Защита документа – Зашифровать с помощью пароля	1

Определите один правильный ответ		
3	Способами совершения преступлений в сфере компьютерной информации являются: а. несанкционированный доступ к файлам законного пользователя б. ввод в систему управления наличными фондами банка ложной информации о перечислении денежных средств в. подключение к телекоммуникативному оборудованию компьютера вопреки воли его владельца г. все ответы правильные	1
Определите один правильный ответ		
4	Протоколирование действий пользователей позволяет а. решать вопросы управления доступом б. реконструировать ход событий при реализации угрозы безопасности информации в. обеспечивать конфиденциальность информации г. восстанавливать утерянную информацию	1
Определите один правильный ответ		
5	Мошенничество, при котором злоумышленники обманным путем выманивают у доверчивых пользователей сети личную информацию, называется: а. крекинг б. грумминг в. фишинг г. биллинг	1
Определите один правильный ответ		
6	Основными субъектами информационной безопасности являются: а. органы права, государства, бизнеса б. руководители, менеджеры, администраторы компаний в. пользователи сети Интернет г. сетевые базы данных, фаерволлы	1
Определите один правильный ответ		
7	К принципам информационной безопасности относятся:	1

	а. постоянный анализ информационного пространства с целью выявления уязвимостей информационных активов б. своевременное обнаружение проблем, потенциально способных повлиять на ИБ в. корректировка моделей угроз и нарушителя г. разработка и внедрение защитных мер д. все ответы верные	
Определите один правильный ответ		
8	Что такое «кибербулинг»? а. запугивание с помощью различных средств информации б. наука о сохранении здоровья при работе со средствами информации в. увеличение производительности веб-приложений за счёт использования сохранённых ранее данных г. взаимодействие между экстремистскими группами в средствах информации	1
Определите один правильный ответ		
9	Что не относится к задачам программно-компьютерной экспертизы? а. расшифровка закодированной информации б. установление формы вины лица, допустившего нарушение правил эксплуатации ЭВМ причинившее существенный вред в. установление авторства файла, программы г. восстановление информации, стертой с физических носителей информации	1
Определите один правильный ответ		
10	Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: а. доступность б. целостность в. актуальность г. конфиденциальность	1
Определите один правильный ответ		

11	Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке: а. Серверные, клиентские, спутниковые, наземные б. Личные, корпоративные, социальные, национальные в. Программные, организационные, клиентские г. Программные, технические, организационные, технологические д. Технические, программные, корпоративные	1
Определите один правильный ответ		
12	Чем известен компьютерный вирус под именем «Чернобыль»? а. блокировал работу компьютеров своим хаотичным и бесконтрольным размножением б. 6 марта форматировал жесткий диск в. 26 апреля активировался, стирал всю информацию на винчестере, повреждал аппаратную часть компьютера г. работал по нарастающей: каждый следующий компьютер отправлял спама еще больше, чем предыдущий	1
Определите один правильный ответ		
13	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков: а. когда риски не могут быть приняты во внимание по политическим соображениям б. для обеспечения хорошей безопасности нужно учитывать и снижать все риски в. когда стоимость контрмер превышает ценность актива и потенциальные потери г. все ответы верны	1
Определите один правильный ответ		
14	Эффективная программа безопасности требует сбалансированного применения: а. контрмер и защитных механизмов б. технических и нетехнических методов в. процедур безопасности и шифрования г. взаимодействия с пользователя системы	1
Определите один правильный ответ		

15	Криптография- это наука, изучающая вопросы а. обеспечения секретности передаваемых сообщений с использованием различных методов б. техники безопасности при работе с компьютером в. шифрования информации г. организации защиты информации физическими методами д. защиты информации от вирусов	1
Определите один правильный ответ		
16	К правовым методам, обеспечивающим информационную безопасность, относятся: а. разработка аппаратных средств обеспечения правовых данных б. разработка и установка во всех компьютерных правовых сетях журналов учета действий в. разработка программных средств г. разработка и конкретизация правовых нормативных актов обеспечения безопасности	1
Определите один правильный ответ		
17	Что не является принципом политики информационной безопасности: а. невозможность миновать защитные средства сети (системы) б. полное блокирование доступа при риск-ситуациях в. усиление защищенности самого незащищенного звена сети (системы) г. разделение доступа (обязанностей, привилегий) клиентам сети (системы)	1
Определите один правильный ответ		
18	Наиболее распространены средства воздействия на сеть офиса: а. слабый трафик, информационный обман, вирусы в интернет б. вирусы в сети, логические мины (закладки), информационный перехват в. компьютерные сбои, изменение администрирования,	1

	топологии г. вирусы в сети, компьютерные сбои	
Определите один правильный ответ		
19	Политика безопасности в системе (сети) – это комплекс: а. нормы информационного права, инструкции поведения б. инструкций, алгоритмов поведения пользователя в сети в. нормы информационного права, соблюдаемые в сети г. руководств, требований обеспечения необходимого уровня безопасности	1
Определите один правильный ответ		
20	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству: а. снизить уровень классификации этой информации б. улучшить контроль за безопасностью этой информации в. требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации г. снизить количество обращений к этой информации	1

МОДУЛЬ 2

Творческая часть (35 баллов)

Задание 1. Когда у мальчика появился телефон с русской клавиатурой (см. рис.) он заметил, что у некоторых его друзей имя и номер телефона «совпадают». Например, Алексей – номер телефона 142-46-24. Определите имя друга мальчика по номеру телефона: 226-16-35.

Ответ: _____

Максимальная оценка за правильно выполненное задание – 15 баллов.

Задание 2. Всмотревшись в текст, найти зашифрованное сообщение (*Максимальная оценка за правильно выполненное задание – 15 баллов*)**:**

криптографиЯ – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данныХ. криптОграфия позволяеТ хранить важную информацию или пЕредавать её по ненадёжным канаЛам связи (таким как интернет) так, что она не может Быть прочитана никем, кроме легитимного получателя. в то время как криптография – это наука о защите даннЫх, *криптоанализ* – это наука об анализировании и взломе зашифрованной Связи. классический крипТоанализ

предствляет сОБой смесь аналитики, математических и статистических расчётОв, а также спокоЙстВия, решительноСТи и удачи. кРиптоаналитиков такжЕ называюТ взломщИками. крипТографическая стойкостЬ измеряетСя тем, сколько понадобитсЯ времени И ресурсОв, чтоБы из шифртекСта восстановить исходный открытый текст. резУльтатом стойкой криптографии является шифртекст, который исключительно сложно взломать без облаДания определённымИ инсТрументами по дешифрованию. но насколько сложно? испоЛьзуя весь вычислительный пОтенциал современной цивилизации – даже миллиардД компьютеров, выполНяющих миллиард Операций в секунду – невозможно Дешифровать рЕзультат стойкой криптографии до конца существования всеЛеннОй.

Ответ: _____

_____

Задание 3. Что такое 1/3 дороги, 3/8 брокколи и 2/5 такси?

	
	

Ответ: _____

Максимальная оценка за правильно выполненное задание – 15 баллов.