Ключи к теоретическим заданиям по профилю «Информационная безопасность»

9 класс

№	Решения и ответы	комментарии
1	а, в, г	1 балл засчитывается только за верный ответ
2	а – убирает сорняки б – собирает помидоры в – моет окна г – убирает помещение	1 балл засчитывается только за верный ответ
3	Решение: (30000 х 100) / (100 – 30) = 42857,15 руб	1 балл засчитывается только за верный ответ
4	в, г, з.	1 балл засчитывается только за верный ответ
5	Управление освещением Управление кондиционированием воздуха (климат контроль) Управление аудио-видео техникой Управление пожарной и охранными сигнализациями	1 балл засчитывается только за верный ответ
6	272	1 балл
7	GDBACEF	4 балла (по 1 баллу за каждые 2 этапа на своём месте)
8	c	2 балла
9	нет	1 балл
10	a	2 балла
11	ab	2 балла(баллы начисляются только если ответ полностью совпадает)
12	RIGHTANSWER	4 балла
13	/etc/shadow	4 балла
14	1) Запрет аутентификации по паролю 2) Смена порта SSH 3) Запрет на вход под учётной записью администратора 4) Настройка сервисов против перебора (fail2ban) 5) Настройка IPS (Intrusion Prevention System)	9 баллов. За каждый способ защиты по 3 балла (максимум 3 способа)
15	1) Настройка WAF (Web Application Firewall) 2) Настройка IPS/IDS 3) Изоляция веб-приложения (контейнер, виртуальная машина) 4) Настройка минимальных разрешения для сервисного пользователя веб-сервера (nginx, apache2) 5) Мониторинг состояния приложения и сервера	9 баллов. За каждый способ защиты по 3 балла (максимум 3 способа)
16	Атака на уязвимость переполнения буфера на стеке заключается в перезаписи адреса возврата или других критичных элементов, расположенных на стеке. Таким образом, перезаписав адрес возврата, можно перенаправить поток выполнения программы в любом русле, например вызвать функцию system или execve для выполнения произвольных команд.	10 баллов

17	a) Хранение паролей “plain text”, в сыром виде – 1 балл b) Хранение паролей с использованием симметричного шифрования (DES) – 3 балла c) Хранение паролей с использованием симметричного шифрования (AES, 3DES, Кузнечик, Магма) – 5 баллов d) Хранение паролей с использованием ассиметричного шифрования (RSA, ГОСТ Р 34.10-2001) – 7 баллов e) Хранение паролей с использованием хэширования (MD4, MD5) – 9 баллов f) Хранение паролей с использованием хэширования и соли (bcrypt, argon2) – 12 баллов	12 баллов
18	Правила: 1. Установка антивирусной программы 2. Использование безопасных и защищенных соединений. 3. При общении не указывать все данные, соблюдать бдительность, не доверять незнакомым, не передавать данные банковской карты 4. Уметь распознавать поддельные сайты. 5. Использовать надежные пароли, разные пароли для разных сайтов. 6. Соблюдать правила общения в сети и др.	10 баллов
19	Потеря телефона при отсутствии пароля: потеря данных (смс, фото, почта), спам-рассылки, вымогательство, потеря денежных средств (доступ к банковским приложениям), доступ ко всем паролям, приложениям	4 балла
20	a	1 балл
21	**Творческое задание.** В ответе должны присутствовать следующие предусмотренные сочетания: 1) номер, срок действия и владелец карты (напечатаны на лицевой стороне карты) – оптический канал – вставление карты в банкомат/получение карты из банкомата – скрытая камера, установленная рядом с банкоматом (допустимо любое иное устройство, позволяющее подсмотреть информацию с лицевой стороны карты, например, так называемый скимер); 2) номер, срок действия и владелец карты – радиоэлектронный канал – совершение операций на экране банкомата – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу, например, так называемый	**25 баллов**

	скимер) или его общее описание; 3) PIN-код – оптический канал – ввод PIN-кода – скрытая камера, установленная рядом с банкоматом (допустимо любое иное устройство, позволяющее подсмотреть информацию с клавиатуры); 4) PIN-код – акустический канал – ввод PIN-кода – подслушивающее устройство, установленное рядом с банкоматом (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш); 5) PIN-код – радиоэлектронный канал – ввод PIN-кода – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу, например, так называемый скимер или его общее описание). • Каждое корректно описанное сочетание: +3 балла. • Перечислены все предусмотренные варианты: +1 балл; • Каждое некорректное сочетание: –2 балла; • Каждое корректное сочетание вне списка предусмотренных: +3 балла ;• Приведено более одного устройства для уже засчитанного сочетания: +1 балл; • Максимальное количество баллов: **25**	
	итого	**100**