Всероссийская олимпиада школьников по технологии школьный этап

8-9 класс

«Информационная безопасность»

2024– 2025 учебный год

*Специальная часть*

*Задание 1.*

Какой нормативно-правовой документ предусматривает наказание за разглашение персональных сведений на территории РФ?

|  |  |
| --- | --- |
|  | Гражданский кодекс Российской Федерации |
|  | Закон РФ «О защите прав потребителей» |
|  | Закон РФ «О государственной тайне» |
|  | **Кодекс Российской Федерации об административных правонарушениях** |
|  | Федеральный закон РФ «Об основах охраны здоровья граждан в Российской Федерации» |

**За верный ответ – 1 балл.**

*Задание 2.*

Установите соответствие между терминами и их определениями

|  |  |  |
| --- | --- | --- |
| **1.**Асимметричное шифрование |  | **А.** это строка символов, которая используется криптографическими алгоритмами для шифрования и расшифровки данных, а также для проверки электронной подписи |
| **2.** Криптография |  | **Б.** способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ |
| **3.** Шифрование |  | **В.** это наука о защите информации с помощью математических методов и алгоритмов |
| **4.**Симметричное шифрование |  | **Г.** это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого |
| **5.** Криптографический ключ |  | **Д.** это метод защиты данных путём их преобразования таким образом, чтобы сообщение могли прочитать только авторизованные пользователи |

Ответ; 1Г, 2В, 3Д, 4 Б, 5А

**За верный ответ – 1 балл.**

**Максимум за задание 5 баллов.**

*Задание 3.*

Вся история развития ЭТОЙ индустрии включает в себя очень много занимательных страниц, однако о самой первой из этих страниц до сих пор ведутся нескончаемые споры. Кто же всетаки придумал ИХ? Когда же появилась самая первая ОНА? Различные источники ссылаются на совершенно различную информацию на этот счет.

Есть такое мнение, что самую первую ЕЁ разработал еще в 1984 году американский программист Энди Хопкинс. Первая ОНА в современном понимании этого термина появилась в 1985 году усилиям Джи Вонга.

Ну, а на отечественном рынке нашим истинным первопроходцем стал Дмитрий Николаевич Лозинский, который разработал ЕЁ в 1988 году, практически одновременно с Макафи.

О чем идет речь в тексте, назовите ЕЁ двумя словами.

Ответ: Антивирусная программа

**За верный ответ – 3 балла.**

*Задание 4.*

Дан список утверждений. Оцените, является ли верным каждое из них

|  |  |  |
| --- | --- | --- |
| Вирусы могут самостоятельно распространяться через сети и заражать другие компьютеры без участия пользователя | **Верно** | Неверно |
| Все киберугрозы можно предотвратить с помощью антивирусного программного обеспечения, и поэтому других мер безопасности не требуется | Верно | **Неверно** |
| Шпионские программы не представляют серьезной угрозы безопасности, так как их цель — просто сбор информации | Верно | **Неверно** |
| Вишинг— вид телефонного мошенничества, нацеленный на получение конфиденциальной информации для доступа к деньгам клиента | **Верно** | Неверно |
| Протоколирование действий пользователей позволяет реконструировать ход событий при реализации угрозы безопасности информации | **Верно** | Неверно |

**За верный ответ – 1 балл.**

**Максимум за задание 5 баллов.**

*Задание 5.*

К какому виду мер защиты информации относится установка автоматических систем пожаротушения и сигнализации?

|  |  |
| --- | --- |
|  | Программным |
|  | Аппаратным |
|  | **Физическим** |
|  | Организационным |

**За верный ответ – 2 балла.**

*Задание 6.*

Какой из следующих методов является наиболее эффективным способом защиты информации от утечки и несанкционированного использования?

|  |  |
| --- | --- |
|  | Использование антивирусных программ |
|  | Регулярное обновление программного обеспечения |
|  | **Криптографическое шифрование информации** |
|  | Очистка кэша браузера |
|  | Дефрагментация дисков, на которых хранится информация |

**За верный ответ – 2 балла.**

*Задание 7.*

Как называется институт гражданского права, защищающий оригинальные произведения искусства, литературы и науки, дающий авторам исключительные права на использование и распространение их трудов?

Ответ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Авторское право)

**За верный ответ – 1 балл.**

*Задание 8.*

С какой периодичностью рекомендуется обновлять ключи шифрования для обеспечения безопасности данных?

|  |  |
| --- | --- |
|  | **Согласно установленному расписанию, а также при определённых обстоятельствах — например, если появляются признаки утечки ключа к нарушителю** |
|  | Один раз в месяц |
|  | При запуске новых криптографических систем |
|  | С периодом времени, не превышающем половину оценочного времени на подбор криптографического ключа нарушителем |
|  | Достаточно обновлять ключи шифрования раз в год |

**За верный ответ – 2 балла.**

*Задание 9.*

Какой способ защиты из перечисленных будет наиболее эффективен для защиты от возможного перебора паролей доступа к системе?

|  |  |
| --- | --- |
|  | Довести до пользователей требования к паролям (длина, комбинация букв, цифр и специальных символов) для повышения их стойкости к перебору |
|  | Отключить сетевой доступ к системе |
|  | Установить ограничения на количество попыток входа – после определенного количества неудачных попыток доступа временно блокировать аккаунт или ввод пароля |
|  | Регулярно менять пароли для всех учётных записей пользователей |
|  | **Использовать двухфакторную аутентификацию – требовать при доступе ввода пароля и sms-подтверждения** |

**За верный ответ – 2 балла.**

*Задание 10.*

Какое сетевое устройство используется для подключения нескольких компьютеров или других устройств в локальной сети?

|  |  |
| --- | --- |
|  | Маршрутизатор/router |
|  | Повторитель/repeater |
|  | **Концентратор/hub** |
|  | Коммутатор/swich |

**За верный ответ – 1 балл.**

*Задание 11.*

Перед вами зашифрованное сообщение, применён шифр простой замены, то есть каждая буква алфавита была заменена во всём тексте какой-то другой буквой того же алфавита.

Ж НТЧЙХЙЦШГЮЙО ЖЕЦ ЦЙЧН ЦЙХЖЙХ МЕТНСЕЙЧ ПРГЬЙЖШГ ФУМНЫНГ, ЦРУЖТУ ИУТЛУТ Ж ЦХЙИТЙЖЙПУЖУС МЕСПЙ; ЖАЖЙИН ЙЗУ НМ ЦЧХУД, СА ФЕХЕРНМШЙС ХЕЁУЧШ ЖЦЙО ЦНЦЧЙСА.

Известно, что в тексте имеется слово «СЕРВЕР».

Как зашифровано слово «СЕРВЕР»?

|  |  |
| --- | --- |
|  | ЖАЖЙИН |
|  | ИУТЛУТ |
|  | **ЦЙХЖЙХ** |
|  | ЦРУЖТУ |
|  | ХЕЁУЧШ |

**За верный ответ – 5 баллов.**

*Задание 12.*

Какое слово зашифровано текстом «МЕТНСЕЙЧ»?

|  |  |
| --- | --- |
|  | СИСТЕМАМ |
|  | КЛЮЧЕВУЮ |
|  | ПОЗИЦИЯМ |
|  | **ЗАНИМАЕТ** |
|  | СЕТЕВЫМИ |

**За верный ответ – 5 баллов.**

*Задание 13.*

Зашифруйте при помощи использованного ключа замены слово «КОММУТАТОР»

|  |  |
| --- | --- |
|  | ФУЖЧУХНЧЙРБ |
|  | **ПУССШЧЕЧУХ** |
|  | ПУТЫЙТЧХЕЧУХ |
|  | ПУССШТНЦЧА |
|  | ПУССЙТЧЕЧУХ |

**За верный ответ – 4 балла.**

*Задание 14.*

Установите соответствие между параметрами URL адреса и примерами:

|  |  |  |
| --- | --- | --- |
| 1.Протокол |  | А. /path/to/resource |
| 2. Доменное имя |  | Б. ?query=parameter |
| 3. Порт |  | В. https://www.dnevnik.ru |
| 4. Путь до ресурса |  | Г. :443 |
| 5. Запрос |  | Д. http:// |

Ответ: 1Д, 2В, 3Г, 4А, 5Б

**За верный ответ – 1 балл.**

**Максимум за задание 5 баллов.**

*Задание 15.*

Этот термин используется в информационной безопасности и программировании. Он обозначает скрытый способ доступа к компьютерной системе или программе, позволяющий обойти стандартные механизмы аутентификации и защиты. Чтобы узнать это слово, реши примеры и выпиши нужные буквы.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | | 2 | 3 | | 4 | 5 | 6 | | 7 | 8 | 9 |
| Т | С | | Б | Р | | Я | Э | Н | | К | Д | О |
|  |  | |  |  | |  |  |  | |  |  |  |
| (123-75)/24 | | (3060/45+2)14 | | | 1257-625\*2 | | 8181/909 -1 | | 72\*9-639 | | 462/42-512/64 | |

Ответ: **БЭКДОР**

**За верный ответ – 2 балла.**

**Кейс задание**

TeslaCrypt - вредоносная программа нацелена, на вспомогательные файлы, связанные с видеоиграми, такие как сохраненные игры, карты, загружаемый контент и тому подобное.

TeslaCrypt распространяются с помощью Angler, Sweet Orange и Nuclear. Данный метод работает следующим образом: пользователь кликает на ссылку, которая ведет к компрометированному (инфицированному) веб-сайту. Это может быть сделано, например, через электронные письма, социальные сети или рекламу.

Как только пользователь открывает сайт, инструменты для эксплуатации уязвимостей начинает работать. Когда браузер загружает страницу, он проверяет есть ли уязвимости в текущей версии браузера или в плагинах, таких как Adobe Flash, Java или Microsoft Silverlight.

Если вредоносные платформы находят уязвимость, они использует её, чтобы запустить скрипт, который загружает вредоносное ПО. После установки TeslaCrypt начинает шифровать файлы на жестком диске и, возможно, на подключенных внешних устройствах. Шифрование осуществляется с использованием сильных алгоритмов, что делает восстановление данных без ключа невозможным.

После завершения шифрования TeslaCrypt отображает сообщение, в котором указывается требуемая сумма выкупа, обычно в биткойнах, и инструкции по оплате. В случае неуплаты выкупа возможность расшифровки файлов теряется навсегда.

А. Выберите виды вредоносных программ и механизмов реализации уязвимостей, которые были упомянуты в приведенном тексте

|  |  |
| --- | --- |
|  | Червь |
|  | Троян |
|  | **Эксплойт** |
|  | Руткит |
|  | SQL-инъекция |
|  | **Вирус-вымогатель** |
|  | Форк-бомба |

Ответ А: (3 балла)

Б. В роли специалиста по информационной безопасности на предприятии, ответе на вопрос: гарантирует ли отключение корпоративной сети от глобальной надежной защиты от этой атаки? Обоснуйте.

Ответ: Нет + обоснование

Участник должен привести обоснования. Например:

*Нет, сотрудник может принести зараженный ноутбук из дома.*

*Отключение от глобальной сети не защищает от физического вмешательства, например, установки вредоносного ПО с помощью USB-накопителей или локальных атак.*

**Правильный ответ без обоснования 0 баллов**

**Правильный ответ с обоснованием 4 балла**

В. Какие меры необходимо предпринять, чтобы не допустить заражения компьютера вредоносной программой TeslaCrypt? Назвать не менее трех мер безопасности.

Ответ: Участник должен упомянуть меры, которые, исходя из описания механизма работы вируса, не дадут ему заразить компьютер. Например:

1. *Регулярно обновлять операционную систему, браузеры и все используемое программное обеспечение. Обновления часто содержат исправления для известных уязвимостей.*
2. *Установить и актуализировать антивирусное программное обеспечение.*
3. *Регулярно создавать резервные копии данных и храните их на внешних устройствах или в облачных сервисах.*
4. *Установить веб-фильтры или решения для предотвращения вредоносного трафика, которые могут блокировать доступ к известным вредоносным сайтам.*
5. *Отключить или удалить ненужные плагины и расширения в браузерах, такие как Adobe Flash и Java, так как они могут содержать уязвимости.*
6. *Проводить обучение для всех пользователей о методах кибербезопасности, включая распознавание фишинговых писем и других потенциально опасных ссылок.*
7. *Настроить программные и аппаратные брандмауэры для защиты сети, чтобы отслеживать и блокировать несанкционированный доступ.*
8. *Настроть права доступа пользователей на компьютере, чтобы минимизировать риск для критически важных файлов и систем. Пользователи должны иметь доступ только к необходимым для работы ресурсам.*

**За каждую меру 1 балл, максимально 3 балла**

**Количество баллов за задание – 10 баллов**