Всероссийская олимпиада школьников по технологии школьный этап

7 класс

«Информационная безопасность»

2024– 2025 учебный год

*Специальная часть*

*Задание 1.*

Цели информационной безопасности – своевременное обнаружение, предупреждение:

|  |  |
| --- | --- |
|  | Компьютерных сбоев |
|  | Инсайдерства в организации |
|  | **Несанкционированного доступа, воздействия в сети** |
|  | Потери информации |
|  | Чрезвычайных ситуаций |

**За верный ответ – 1 балл.**

*Задание 2.*

Основная масса угроз информационной безопасности приходится на:

|  |  |
| --- | --- |
|  | Рекламные программы |
|  | Шпионские программы |
|  | Черви |
|  | **Троянские программы** |
|  | Программы мутанты |

**За верный ответ – 1 балл.**

*Задание 3.*

Когда получен спам по e-mail с приложенным файлом, следует:

|  |  |
| --- | --- |
|  | **Удалить письмо с приложением, не раскрывая (не читая) его** |
|  | Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама |
|  | Прочитать приложение, если оно не содержит ничего ценного – удалить |
|  | Главное не загружать письмо, читать можно |

**За верный ответ – 1 балл.**

*Задание 4.*

С какими из приведенных ниже примеров угроз вы можете столкнуться в Интернете? Укажите все верные варианты.

|  |  |
| --- | --- |
|  | **Вирусы** |
|  | **Вредоносные ПО** |
|  | Сетевые протоколы |
|  | **Фишинг** |
|  | Хэш-функции |

**За полностью верный ответ – 1 балл.**

*Задание 5.*

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

|  |  |  |
| --- | --- | --- |
| Создание бэкапов (резервных копий) данных способно предотвратить их потерю и восстановить исходные данные при необходимости. | **Верно** | Неверно |
| Шифр и пароль – это слова антонимы | Верно | **Неверно** |
| Троянский конь – это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Telegram, телефон и т.п. | Верно | **Неверно** |
| Нажатие на рекламу и всплывающие окна в интернете может привести к заражению вашего компьютера вредоносными программами | **Верно** | Неверно |
| Новые виды вирусов и вредоносного ПО появляются постоянно, а лучшей защитой от них является регулярное обновление рабочего и антивирусного ПО | **Верно** | Неверно |

**За верный ответ – 0.4 балла.**

**Максимум за задание 2 балла.**

*Задание 6.*

Какой из паролей, приведенных ниже, является самым защищенным от атак (сильным паролем)?

|  |  |
| --- | --- |
|  | 1234567 |
|  | qwerty |
|  | **MG&d\_m@S4** |
|  | Степан12 |
|  | MG&d |

**За верный ответ – 2 балла.**

*Задание 7.*

Какого метода защиты информации не существует? Укажите все верные варианты

|  |  |
| --- | --- |
|  | **Шифрование** |
|  | **Аппаратные методы защиты** |
|  | **Программные методы защиты** |
|  | **Резервное копирование** |
|  | Дезинфекция |

**За верный ответ – 1 балл.**

**Максимум за задание 4 балла.**

*Задание 8.*

Какие последствия возможны при несанкционированной утечке информации? Укажите все верные варианты.

|  |  |
| --- | --- |
|  | Снижение затрат на безопасность |
|  | **Нарушение работоспособности оборудования и/или ПО** |
|  | **Финансовые убытки** |
|  | **Потеря данных** |
|  | **Ущерб репутации** |

**За верный ответ – 1 балл.**

**Максимум за задание 4 балла.**

*Задание 9.*

Установите соответствие между терминами и их определениями

|  |  |  |
| --- | --- | --- |
| **1.** Спам |  | **А.** Использование психологических манипуляций для получения доступа к конфиденциальной информации |
| **2.** Криптография |  | **Б.** Протокол прикладного уровня передачи данных в формате HTML, использующийся для получения информации с веб-сайтов |
| **3.** Аутентификация |  | **В.** Наука о защите информации с помощью математических методов и алгоритмов |
| **4.** HTTP |  | **Г.** Массовая рассылка рекламы при помощи электронной почты или программ |
| **5.**Социальная инженерия |  | **Д.** проверка личности пользователя с помощью процедуры проверки (например, сравнение введенных логина и пароля с логином и паролем, находящимися в базе данных) |

Ответ:1Г, 2В, 3Д, 4Б, 5А

**За верный ответ – 1 балл.**

**Максимум за задание 5 баллов.**

*Задание 10.*

Для удобства продажи автобусных билетов на автовокзале города N планируют установить терминалы самообслуживания. Пассажиру для приобретения билета потребуется самостоятельно ввести при помощи экранной клавиатуры и встроенного сканера дату отправления и номер автобуса, выбрать место, отсканировать документы, дающие право на приобретение льготного билета, после чего осуществить оплату банковской картой, вставив её в соответствующий разъём терминала и введя PIN-код. Оцените, какие из утверждений являются верными, а какие нет.

|  |  |  |
| --- | --- | --- |
| Для сведений о наличии свободных мест в автобусе потребуется обеспечить доступность | **Верно** | Неверно |
|  | Верно | Неверно |
| Пассажиры, покупающие билеты, могут рассматриваться как возможные нарушители информационной безопасности терминалов | **Верно** | Неверно |
| Отключение терминала от электропитания будет являться нарушением целостности | Верно | **Неверно** |
| Для вводимых данных покупателя потребуется обеспечивать конфиденциальность | **Верно** | Неверно |

**За верный ответ – 1 балл.**

**Максимум за задание 5 баллов.**

*Задание 11.*

Дополните следующее утверждение, выбрав правильный вариант ответа

Смишинг – это вид мошенничества, заключающийся в том, что злоумышленник пытается получить у жертвы конфиденциальную информацию посредством использования социальной инженерии и средств…

|  |  |
| --- | --- |
|  | Видеоконференций |
|  | Телефонной коммуникации |
|  | **SMS-сообщений или мессенджеров** |
|  | Почтовой коммуникации |
|  | Социальных сетей |

**За верный ответ – 1 балл.**

*Задание 12.*

Перед вами сообщение, зашифрованное шифром Цезаря. При шифровании был использован русский алфавит. Определите значение сдвига (наименьшее значение) и расшифруйте сообщение.

Зашифрованное сообщение:

ЕИФИЖМХА ЕИЗ, УТОД МЩ СИЦ

Ответ: Значение сдвига = 4, Берегись бед, пока их нет (10 баллов в сумме)

**Правильно расшифрованное сообщение 7,5 баллов**

**Правильно указанное значение сдвига 2,5 балла**

*Задание 13.*

Зашифруйте с тем же сдвигом слово «ПАРОЛЬ».

|  |  |
| --- | --- |
|  | шзхуме |
|  | ъхетнч |
|  | жцйзие |
|  | **фехурб** |
|  | цйпхйч |

**За верный ответ – 3 балла.**

*Задание 14.*

Сотрудники полиции столкнулись с новой хакерской группировкой, которая атакует правительственные сайты. Для того, чтобы раскрыть их, 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 | 728 |
| Технические навыки | 505 |
| Социальная инженерия | технические навыки | 947 |

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

Ответ: **286**

**За верный ответ – 5 баллов.**

Решение:

Для вычисления количества хакеров, которые владеют и социальной инженерией, и техническими навыками, можно воспользоваться формулой для объединения множеств и учитывать пересечение:

1. Обозначим:

- A = хакеры, владеющие социальной инженерией (728)

- B = хакеры, владеющие техническими навыками (505)

- A ∪ B = хакеры, владеющие либо социальной инженерией, либо техническими навыками (947)

2. Используем формулу для объединения множеств:

|A ∪ B| = |A| + |B| - |A ∩ B|

где |A ∩ B| - это количество хакеров, обладающих и социальной инженерией, и техническими навыками.

3. Подставим известные значения в формулу:

947 = 728 + 505 - |A ∩ B|

4. Упростим уравнение:

|A ∩ B| = 728 + 505 - 947

|A ∩ B| = 1233 - 947

|A ∩ B| = 286

Таким образом, количество хакеров, владеющих и социальной инженерией, и техническими навыками, составляет 286

**Кейс задание**

Первая крупная афера с помощью имитации голоса произошла в Великобритании. Жертвой мошенников стал гендиректор британской энергетической фирмы.

Мошенники позвонили и, подменив голос, успешно выдали себя за немецкого генерального директора материнской компании британской энергетической компании. Вызов определился как звонок из головного офиса немецкой компании, не вызывав подозрений. Мужчина разговаривал по телефону с вышестоящим лицом, исполнительным директором немецкой головной компании. Голос в трубке был с узнаваемым акцентом, он попросил в течение часа перечислить 243 тысячи долларов на счет венгерскому поставщику, который, по сути, был счетом преступников. Подчиненный ничего не заподозрил и деньги перечислил. Мошенникам этого показалось мало, и они решили запросить еще один перевод, хакеры позвонили снова. Однако британский директор уже начал подозревать неладное и не согласился провести платеж.

А. Выберите техники реализации угроз информационной безопасности из списка ниже, которые однозначно были использованы в приведенном эпизоде (исходя из приведенного описания инцидента)

|  |  |
| --- | --- |
|  | Фишинг |
|  | Тайпсквоттинг |
|  | Инъекция |
|  | **Спуфинг** |
|  | Несанкционированный доступ |
|  | **Вишинг** |

**Ответ А: (3 балла)**

Б. Является ли приведенный эпизод примером использования механизмов социальной инженерии? Ответ обоснуйте.

**Ответ Б:** Да, является. Участник должен привести в качестве обоснования пример механизма социальной инженерии из приведенного эпизода. Например:

*Да, является, потому что злоумышленники подменили голос при помощи ИИ, и выдали себя за другого человека с целью мошенничества, а это вишинг.*

*Да, потому путем подмены телефонного номера, в диалоге по телефону убеждали жертву перевести деньги, а это спуфинг.*

**Правильный ответ без обоснования** (0 баллов)

**Правильный ответ с обоснованием** (4 балла)

В. Укажите, что требуется (не) делать пользователям услуг связи, чтобы не стать жертвой подобного рода мошенничества?

Ответ В: (3 балла)

Участник должен упомянуть как минимум одну профилактическую меру или превентивный механизм против методов социальной инженерии из эпизода, например:

1. Не переводить денежные средства на счета пользователей, с которыми вы не знакомы / не доверенным лицам.

2. Проверять личность звонящего контрольными вопросами / просьбой предоставить данные или иной элемент для проверки подлинности звонящего.

3. Проверка источника звонка или звонок в структуру, способную подтвердить (верифицировать) запрос, например, оператору связи или в головную компанию.

**Количество баллов за все задание – 10 баллов**