МАТЕРИАЛЫ ЗАДАНИЙ МЕЖРЕГИОНАЛЬНОЙ ОЛИМПИАДЫ ШКОЛЬНИКОВ ИМЕНИ И.Я. ВЕРЧЕНКО ПО ПРОФИЛЮ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ» (2024/2025 УЧЕБНЫЙ ГОД)

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП 8-10 КЛАССЫ

Задача 1. Система защиты

Вариант 1

В компании используется система защиты от DDoS-атак, основанная на анализе активности пользователей. Система анализирует журнал активности пользователей, в котором вычисляет количество запросов от уникальных пользователей в единицу времени. Журналы содержат информацию о попытках доступа к серверу, включая IP-адреса пользователей, с которых осуществлялось обращение. Если количество одновременных подключений разных пользователей превышает пороговое значение, выдается предупреждение о возможной DDoS-атаке.

Перед запуском системы необходимо её настроить (обучить) на корректном трафике. Для этих целей был подготовлен журнал запросов от сотрудников компании за определенный период времени.

Определите, какое максимальное количество одновременных подключений разных пользователей в минуту необходимо установить в системе защиты, чтобы она корректно работала и не выдавала ложных предупреждений. Разработчики рекомендуют устанавливать пороговое значение на 10% больше максимально возможного числа подключений в единицу времени.

В ответе укажите само пороговое значение (количество подключений в единицу времени), а также обоснование выбранного значения.

К задаче прилагается:
файл «log_v1.log» – журнал посещений

Вариант 2

В компании используется система защиты от DDoS-атак, основанная на анализе активности пользователей. Система анализирует журнал активности пользователей, в котором вычисляет количество запросов от уникальных пользователей в единицу времени. Журналы содержат информацию о попытках доступа к серверу, включая IP-адреса пользователей, с которых осуществлялось обращение. Если количество одновременных подключений разных пользователей превышает пороговое значение, выдается предупреждение о возможной DDoS-атаке.

Перед запуском системы необходимо её настроить (обучить) на корректном трафике. Для этих целей был подготовлен журнал запросов от сотрудников компании за определенный период времени.

Определите, какое максимальное количество одновременных подключений разных пользователей в минуту необходимо установить в системе защиты, чтобы она корректно работала и не выдавала ложных предупреждений. Разработчики рекомендуют устанавливать пороговое значение на 10% больше максимально возможного числа подключений в единицу времени.

В ответе укажите само пороговое значение (количество подключений в единицу времени), а также обоснование выбранного значения.

К задаче прилагается:
файл «*log_v2.log*» – журнал посещений

Задача 2. Контрольная выборка атак

Вариант 1

На сервер зафиксировано 150 атак. Из них:
- 60 сетевых атак (20 произошли в первой половине дня, 40 во второй),
- 40 атак на приложения (15 критических и 25 некритических),
- 50 системных атак (32 произошли в первой половине дня, 18 во второй).

Для обучения системы безопасности необходимо выбрать 20 атак для анализа так, чтобы:
- среди них было ровно 10 сетевых атак, 3 в первой половине, 7 во второй половине дня;
- 5 атак на приложения обязательно должны быть критическими;
- 5 атак должны быть системными, из которых 2 атаки произошли во второй половине дня.

Сколько различных наборов таких обучающих выборок может быть получено? Ответ обоснуйте.

Вариант 2

На сервер зафиксировано 200 атак. Из них:
- 80 сетевых атак (30 произошли в первой половине дня, 50 во второй),
- 70 атак на приложения (20 критических и 50 некритических),
- 50 системных атак (30 произошли в первой половине дня, 20 во второй).

Для обучения системы безопасности необходимо выбрать 20 атак для анализа так, чтобы:

– среди них было ровно 12 сетевых атак, 4 в первой половине, 8 во второй половине дня;
– 6 атак на приложения обязательно должны быть критическими;
– 2 атаки должны быть системными, из которых 1 атака произошла во второй половине дня.

Сколько различных наборов таких обучающих выборок может быть получено? Ответ обоснуйте.

Задача 3. Таблица символов

Вариант 1

В ходе анализа содержимого персонального компьютера была обнаружена таблица символов (таблица 1) и скриншот формулы (рисунок 1).

Экспертами установлено, что в таблице символов скрыт пароль от рабочего стола компьютера, каждая буква которого находится на определенной позиции, вычисляемой с помощью указанной формулы.

Определите пароль, если известно, что координаты первого символа: $(x_0, y_0) = (6, 9)$, длина пароля – *13* символов, и пароль является осмысленным словом. В ответе укажите сам пароль и значения параметров формулы.

Таблица 1 – Таблица символов

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
1	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	О	Ю
2	Я	А	Б	В	Г	Н	Е	Ё	Ж	З	И	Й	К	Л	М	Н
3	О	П	Р	С	Т	У	Ф	Ч	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
4	Ю	Я	А	Я	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
5	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ц	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л
7	М	Н	О	П	Р	С	Т	У	Н	Х	Ц	Ч	Ш	Щ	Ъ	Ы
8	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	Е
9	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
10	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	И	И	Й
11	К	Л	М	Н	С	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
12	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	О	Ё	Ж	З	И
13	Й	К	Е	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
14	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	Т	Т	Д	Е	Ё	Ж	З
15	Л	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч

$$x_{i+1} = (x_i + a)\ mod\ 16, \qquad y_{i+1} = (y_i + b)\ mod\ 16$$

Рисунок 1 – Формулы вычисления координат символов,
mod – операция остатка от деления

Вариант 2

В ходе анализа содержимого персонального компьютера была обнаружена таблица символов (таблица 1) и скриншот формулы (рисунок 1).

Экспертами установлено, что в таблице символов скрыт пароль от рабочего стола компьютера, каждая буква которого находится на определенной позиции, вычисляемой с помощью указанной формулы.

Определите пароль, если известно, что координаты первого символа: $(x_0, y_0) = (4, 6)$, длина пароля – *14* символов, и пароль является осмысленным словом. В ответе укажите сам пароль и значения параметров формулы.

Таблица 1 – Таблица символов

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	О	Ф	У	Т	С	Р
1	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	В	Б
2	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	И	Ч	Ц	Х	Ф	У	Т	С
3	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	О
4	Б	А	Я	Ю	Э	Ь	О	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т
5	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Т	Д	Г
6	В	Б	А	Я	П	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У
7	Т	С	Р	П	О	Н	М	Л	К	Й	И	Е	Ж	Ё	Е	Д
8	Г	В	Я	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф
9	У	Т	С	Р	П	О	Н	М	Л	С	Й	И	З	Ж	Ё	Е
10	И	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х
11	Ф	У	Т	С	Р	П	О	Р	М	Л	К	Й	И	З	Ж	Ё
12	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц
13	Х	Ф	У	Т	С	Н	П	О	Н	М	Л	К	Й	И	З	Ж
14	Ё	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Т	Щ	Ш	Ч
15	Ц	Х	Ф	В	Т	С	Р	П	О	Н	М	Л	К	Й	И	З

$$x_{i+1} = (x_i + a)\ mod\ 16, \qquad y_{i+1} = (y_i + b)\ mod\ 16$$

Рисунок 1 – Формулы вычисления координат символов,
mod – операция остатка от деления

Задача 4. Исходный код

Вариант 1

В связи с усилением требований к защите данных, руководство компании решило разработать алгоритм шифрования для безопасной передачи сообщений, которая должна шифровать конфиденциальные данные перед отправкой по сети. Алгоритм основан на принципе блочного шифрования и работает с текстами фиксированной длины в байтах.

Разработчики по ошибке опубликовали код функции шифрования в публичном репозитории (листинг 1). Зная исходный код и перехваченные зашифрованные данные определите исходное сообщение. В ответе укажите исходное сообщение и обоснуйте алгоритм дешифрования.

Зашифрованное сообщение:

```
122 72 127 124 81 93 96 122 81 74 65 117 91 85 113 94 118 170 170
```

Листинг 1. Функция шифрования на различных языках программирования

Python

```
def encrypt(text, key):
  encrypted = []
  for i, char in enumerate(text):
    encrypted.append(
        (ord(char)+i)^key )
  return encrypted
```

C

```
char* encrypt(char* text, char key)
{
  char *encrypted = new char[strlen(text)+1];
  for (int i  = 0; i < strlen(text); i++)
    encrypted[i] = (text[i] + i) ^ key;
  encrypted[strlen(text)] = '\0';
  return encrypted;
}
```

C++

```
std::string encrypt(std::string text, char key)
{
  std::string encrypted = "";
  for (int i = 0; i < text.length(); i++)
    encrypted[i] = (text[i] + i) ^ key;
  return encrypted;
}
```

Вариант 2

В связи с усилением требований к защите данных, руководство компании решило разработать алгоритм шифрования для безопасной передачи сообщений, которая должна шифровать конфиденциальные данные перед отправкой по сети. Алгоритм основан на принципе блочного шифрования и работает с текстами фиксированной длины в байтах.

Разработчики по ошибке опубликовали код функции шифрования в публичном репозитории (листинг 1). Зная исходный код и перехваченные зашифрованные данные определите исходное сообщение. В ответе укажите исходное сообщение и обоснуйте алгоритм дешифрования.

Зашифрованное сообщение:

```
99 81 102 101 72 68 89 99 72 106 64 106 66 125 77 76 111 69
```

Листинг 1. Функция шифрования на различных языках программирования

Python

```
def encrypt(text, key):
  encrypted = []
  for i, char in enumerate(text):
    encrypted.append(
        (ord(char)+i)^key )
  return encrypted
```

C

```
char* encrypt(char* text, char key)
{
  char *encrypted = new char[strlen(text)+1];
  for (int i  = 0; i < strlen(text); i++)
    encrypted[i] = (text[i] + i) ^ key;
  encrypted[strlen(text)] = '\0';
  return encrypted;
}
```

C++

```
std::string encrypt(std::string text, char key)
{
  std::string encrypted = "";
  for (int i = 0; i < text.length(); i++)
    encrypted[i] = (text[i] + i) ^ key;
  return encrypted;
}
```

Задача 5. Обфускация

Вариант 1

На компьютере хакера нашли фрагменты вредоносного кода. Автор обфусцировал весь исходный код. В ходе анализа был определен фрагмент функции аутентификации (листинг 1), которая возвращает `'True'` при успешном вводе пароля и запускает другие фрагменты кода.

Определите, какое секретное слово необходимо ввести, чтобы обнаруженный фрагмент аутентификации вернул `'True'`. Ответ обоснуйте.

Листинг 1. Фрагмент функции аутентификации

Python

```
exec('dAzD chjhQwek_sjhQweryuSWbE(sjhQweryuSWbE):\n    ryuSWbEurn
sjhQweryuSWbE[:17] ==  "Ha[3m[3mYNioskjear_" + c(487tHH0) + c(42)(48) +
c(487tHH0) +
c(487tHH3)\n[3mrinthE(chjhQwek_sjhQweryuSWbE(sjhQweryuSWbE))\n'.replace('87tHH',
'2)(5').replace('yuSWb', 'eth').replace('ioskj', 'ewY').replace('(42)',
'hr').replace('AzD', 'ef').replace('qQT', 'ut').replace('[3m',
'p').replace('jhQwe', 'ec').replace('thE', 't'), {'secret': input()})
```

Вариант 2

На компьютере хакера нашли фрагменты вредоносного кода. Автор обфусцировал весь исходный код. В ходе анализа был определен фрагмент функции аутентификации (листинг 1), которая возвращает `'True'` при успешном вводе пароля и запускает другие фрагменты кода.

Определите, какое секретное слово необходимо ввести, чтобы обнаруженный фрагмент аутентификации вернул `'True'`. Ответ обоснуйте.

Листинг 1. Фрагмент функции аутентификации

Python

```
exec('djhQwe chAzDk_sAzDryuSWbE(sAzDryuSWbE):    \n    ryuSWbEurn
sAzDryuSWbE[:18] ==  "MerioskjhrqQTt[3(42)" + chr(50) + chr(48) + chr(50) +
chr(53)\nprinthE(chAzDk_sAzDryuSWbE(sAzDryuSWbE))\n'.replace('87tHH',
'2)(5').replace('yuSWb', 'eth').replace('ioskj', 'ryC').replace('(42)',
'mas').replace('AzD', 'ec').replace('qQT', 'is').replace('[3m',
'hEm').replace('jhQwe', 'ef').replace('thE', 't'), {'secret': input()})
```