ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»

Московский конкурс межпредметных навыков и знаний
«Интеллектуальный мегаполис. Потенциал»

Методические рекомендации
для подготовки к практическому этапу
в номинации «ИТ-класс»
по направлению Информационная безопасность и технологии связи
2024-2025 учебный год

Москва 2024

Содержание

Спецификация конкурсных материалов
для проведения *практического* этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» в номинации «*ИТ-класс*» по направлению *Информационная безопасность и технологии связи*

1. Назначение конкурсных материалов

Материалы *практического* этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» (далее – Конкурс) предназначены для оценки уровня *практической* подготовки участников Конкурса.

2. Условия проведения

Практический этап Конкурса проводится в очном дистанционном формате с использованием технологии прокторинга. Участникам необходимо иметь компьютер (ПК или ноутбук; прохождение диагностики на мобильных устройствах - невозможно) с выходом в Интернет, веб-камерой и микрофоном, а также смартфон (или планшет) со стабильным интернетом и приложением для считывания QR-кодов. Требуется предварительная настройка оборудования: https://im.mcko.ru/docs/Инструкция_для_участника_конкурса_Интеллектуальный_мегаполис_Потенциал.pdf . Браузер разрешается использовать только для прохождения заданий этапа и процедуры прокторинга.

Дополнительное ПО, разрешенное для прохождения: текстовый редактор, графический редактор, MS Excel, электронные таблицы (как обычный калькулятор, исключая специализированные формулы), обычный встроенный калькулятор, компилятор, установленный на компьютере, онлайн-компилятор.

Чем пользоваться категорически нельзя (ведет к отклонению работы): веб-поиском, методическими указаниями.

3. Продолжительность выполнения

На выполнение заданий *практического* этапа Конкурса отводится 120 минут. Во время проведения мероприятия участник может выйти из зоны проведения

мероприятия не более чем на 5 минут, предупредив *проктора на камеру*. Мероприятие не продлевается на время отсутствия участника.

4. Содержание и структура

Индивидуальный вариант участника включает *11* заданий, базирующихся на содержании *элективного курса "Введение в ИТ-специальность".*

5. Система оценивания

Задание считается выполненным, если ответ участника совпал с эталоном. Максимальный балл за выполнение 10 заданий – 60 баллов.

6. Приложения

1. План конкурсных материалов для проведения *теоретического* этапа Конкурса.
2. Демонстрационный вариант конкурсных заданий *теоретического* этапа Конкурса.
3. Критерии оценки заданий.
4. Пример решения задач.
5. Список учебной и методической литературы и другие источники.

Приложение 1

Московский конкурс межпредметных навыков и знаний
«Интеллектуальный мегаполис. Потенциал»

План конкурсных материалов для проведения практического этапа Конкурса

№ задания	Выбор задания для решения	Уровень сложности	Уникальные кодификаторы Конкурса	Контролируемые требования к проверяемым умениям	Балл
1.	-	*базовый*	4.1.6. Доменная система имен	Умение применять иерархию доменов. Умение соотносить доменное имя и IP-адрес. Умение применять роли и функции DNS-серверов.	4
2.	-	*базовый*	4.1.7. IP-адресация	Умение применять IP-адресацию, умение назначать маски подсетей.	4
3.	-	*базовый*	4.1.8. Расчет количества компьютеров в сети	Умение рассчитывать количество хостов в сети	4
4.	4, 5	*повышенный*	4.2.7. Запросы к базам данных	Умение осуществлять запрос к базе данных	8
5.	4, 5	*повышенный*	4.3.2. Основы операционной системы Linux	Умение применять командную строку Linux, осуществлять поиск текстовой информации в файлах	
6	-	*повышенный*	4.1. Основы защиты информации	Умение применять основы защиты информации, применять алгоритмы шифрования	8
7.	-	*базовый*	4.1.4 Файловая система, интерфейс командной строки	Умение ориентироваться в файловой системе, выполнять	4

				простейшие команды в ОС Windows/Linux	
8.	-	*базовый*	4.3.2 Основы операционной системы Linux	Умение ориентироваться в файловой системе, выполнять простейшие команды в ОС Windows/Linux	4
9.	-	*повышенный*	4.2.4 Практика работы с интерфейсами	Умение анализировать и интерпретировать результаты сканирования ресурсов сети	8
10.	-	*повышенный*	4.1.8 Расчет количества компьютеров в сети	Умение эффективно управлять ресурсами сети	8
11.	-	*повышенный*	4.1 Основы защиты информации	Умение применять алгоритмы хэширования в задачах криптографии	8
				Сумма баллов:	**60**

Приложение 2

МТУСИ

Московский конкурс межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал»

Демонстрационный вариант конкурсных заданий практического этапа Конкурса.

(Задания: 7, 8, 9, 10, 11)

Задание 7.

Злоумышленник получил несанкционированный доступ к одному из компьютеров внутри корпоративной сети компании. Злоумышленнику необходимо узнать IP-адреса всех сетевых интерфейсов этого компьютера, а также другую информацию, которая поможет ему в дальнейшем анализе и атаках. Какую команду в командной строке Windows злоумышленник может использовать, чтобы вывести подробную информацию обо всех сетевых интерфейсах компьютера, включая IP-адреса, маски подсети, шлюзы, DNS-серверы и другие сетевые параметры?

Ответ: ipconfig /all

Задание 8.

Вы системный администратор компании, и у вас есть права администратора (root-права) на одном из ключевых серверов. Сервер работает под управлением операционной системы Linux. Согласно политике безопасности компании, все SSH-соединения должны быть ограничены, и любые новые или несанкционированные соединения могут указывать на потенциальное нарушение безопасности. Во время регулярного мониторинга вы обнаружили одно активное SSH-соединение, которое не было авторизовано. Это указывает на возможный несанкционированный доступ к серверу. Ваша задача — найти и немедленно разорвать это соединение, чтобы предотвратить дальнейшие нарушения.

Список активных соединений указан ниже:

Proto	Local Address	Foreign Address	State	PID
TCP	192.168.1.10:80	192.168.1.200:54321	ESTABLISHED	1001
TCP	192.168.1.10:22	192.168.1.200:56789	ESTABLISHED	1010
TCP	192.168.1.10:23	192.168.1.200:48321	ESTABLISHED	1011
TCP	192.168.1.10:443	192.168.1.200:56768	ESTABLISHED	1101
TCP	192.168.1.10:21	192.168.1.200:67890	ESTABLISHED	1201
TCP	192.168.1.10:25	192.168.1.200:78901	ESTABLISHED	1302
TCP	192.168.1.10:53	192.168.1.200:89012	ESTABLISHED	1421
TCP	192.168.1.10:143	192.168.1.200:54123	ESTABLISHED	1454
TCP	192.168.1.10:989	192.168.1.200:57632	ESTABLISHED	1045

Напишите команду, которая завершит процесс, связанный с несанкционированным SSH-соединением.

Ответ: kill 1010

Задание 9.

Компания «Протект» управляет крупной распределенной сетью умных устройств, подключенных к интернету (IoT). Эти устройства установлены на множестве удаленных объектов, и они критически важны для операций компании, включая мониторинг и управление производственными процессами. В последнее время в компании возникли опасения по поводу возможных уязвимостей в этих устройствах, особенно тех, которые не были обновлены до последних версий прошивки. Ваша задача — выполнить аудит безопасности сети, чтобы выявить все активные устройства и определить, какие из них работают на устаревших или уязвимых версиях программного обеспечения. Для выполнения поставленной задачи вы решили воспользоваться функционалом сканера сети «nmap».

Какой командой nmap вы можете просканировать сеть 192.168.50.0/24, чтобы обнаружить все активные устройства и попытаться определить версии их программного обеспечения, чтобы выявить потенциально уязвимые устройства?

Ответ. nmap -sP -sV 192.168.50.0/24

Задание 10.

В компании "ИНФОСекьюрити" произошел инцидент информационной безопасности, связанный с неправомерным доступом к конфиденциальным данным. В связи с этим руководство компании приняло решение усилить защиту сети путем ее сегментации с использованием VLAN. Это позволит изолировать различные отделы и снизить риски утечек данных.

Администратор сети должен настроить следующие VLAN:

1. VLAN A (Отдел разработки): Необходимо обеспечить подключение до 500 устройств.

2. VLAN B (Отдел маркетинга): Необходимо обеспечить подключение до 200 устройств.

3. VLAN C (Финансовый отдел): Необходимо обеспечить подключение до 30 устройств.

Необходимо определить, какую минимальную маску подсети нужно использовать для каждой из указанных VLAN (A, B и C) и сколько всего IP-адресов будет выделено для всех подсетей вместе?

Ответ необходимо записать в следующем формате «A:/??, B:/??, C:/?? Количество IP-адресов: ??».

Ответ: A:/23, B:/24, C:/27 Количество IP-адресов: 800

Задание 11.

Администратор системы защиты информации компании забыл свой пароль от центра управления системами безопасности, который отвечает за мониторинг и управление всей инфраструктурой безопасности. К счастью, у администратора сохранилось хеш-значение правильного пароля, а также список из 10 паролей, которые он обычно использует. Один из этих паролей точно является правильным, но его необходимо определить.

Хеш-значение, вычисляемое при вводе последней буквы пароля, становится хеш-значением всего пароля. Для вычисления хеш-значений паролей в системе используется следующая формула:

$H_i=(H_{(i-1)}+M_i)^2 \bmod n$

где: H0 = 5 - начальный вектор инициализации, Mi - значение i-й буквы в пароле (номер буквы в алфавите), mod n – операция взятия остатка от деления на n, n = 187.

Хеш-значение правильного пароля – 26

Список паролей для проверки представлен ниже:

1	КОЛЛИЗИЯ
2	ПРОКСИФИКАЦИЯ
3	БЕЗОПАСНОСТЬ
4	АНАЛИТИК
5	СИСТЕМА
6	КРИПТОСТОЙКОСТЬ
7	АДМИНИСТРИРОВАНИЕ
8	УПРАВЛЕНИЕ
9	ПРЕОБРАЗОВАНИЕ
10	КЛАССИФИКАТОР

Алфавит, используемый при вычислении хеш-значения:

Буква	А	Б	В	Г	Д	Е	Ё	Ж
Позиция в алфавите	1	2	3	4	5	6	7	8
Буква	З	И	Й	К	Л	М	Н	О
Позиция в алфавите	9	10	11	12	13	14	15	16
Буква	П	Р	С	Т	У	Ф	Х	Ц
Позиция в алфавите	17	18	19	20	21	22	23	24
Буква	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю
Позиция в алфавите	25	26	27	28	29	30	31	32
Буква	Я							
Позиция в алфавите	33							

Напишите программу, которая для каждого из предложенных паролей вычисляет его хеш-значение и сравнивает его с правильным значением (26). В ответе укажите пароль, хеш которого совпадает с данным значением.

Ответ: КРИПТОСТОЙКОСТЬ

Приложение 3

Московский конкурс межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал»

Критерии оценки заданий практического этапа Конкурса (Задания: 7, 8, 9, 10, 11)

Задания: 7, 8, 9, 10, 11

Баллы	Уровень сложности	Критерии оценки
0	Базовый/повышенный	Дан неверный ответ, не предоставлен правильный ответ на задание.
4	базовый	Дан правильный ответ и представлено полное и логичное решение.
8	повышенный	Дан правильный ответ и представлено полное и логичное решение.

Приложение 4

Московский конкурс межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал»

Пример решения задач практического этапа Конкурса (Задания: 7, 8, 9, 10, 11)

<table>
<tr><th>Номер задания</th><th>Решение</th><th>Ответ</th></tr>
<tr><td>Задание 7.</td><td>Команда ipconfig /all позволяет получить детальную информацию обо всех сетевых интерфейсах. Эта команда выводит IP-адреса, маски подсети, шлюзы, DNS-серверы и другие параметры конфигурации сети, что помогает в дальнейшем анализе сети и потенциальных атаках.
Альтернативные команды, такие как netsh interface ip show config, также могут предоставить информацию о сетевых интерфейсах, включая IP-адреса и шлюзы, но не столь детализированную, как ipconfig /all. Команда netstat -r может быть использована для получения данных о маршрутах и шлюзах, но её функциональность ограничена относительно общего вывода информации о конфигурации интерфейсов. Таким образом, ipconfig /all остаётся наиболее полной и эффективной командой для получения сетевых данных в рассматриваемом сценарии.</td><td>ipconfig /all</td></tr>
<tr><td>Задание 8.</td><td>Для решения этой задачи необходимо проанализировать таблицу представленных активных соединений. Далее необходимо найти информацию о несанкционированном SSH-соединении.
SSH-соединение обычно работает через порт 22 (протокол TCP). В предоставленном списке активных соединений одно из соединений использует этот порт:
<table><tr><td>TCP</td><td>192.168.1.10:22</td><td>192.168.1.200:56789</td><td>ESTABLISHED</td><td>1010</td></tr></table>
Согласно условию задачи политикой безопасности SSH-соединения ограничены, но не запрещены. Чтобы немедленно разорвать SSH-соединение используется команда kill, которая завершает процесс по его PID (идентификатору процесса) будет: kill 1010</td><td>kill 1010</td></tr>
<tr><td>Задание 9.</td><td>Для выполнения поставленной задачи по аудиту безопасности сети, использующей IoT-устройства, ключевым аспектом является выявление всех активных устройств в сети и определение версий их программного обеспечения. Из условия задачи следует воспользоваться сканером сети nmap, который позволяет обнаруживать устройства в сети и получать информацию о версиях их программного обеспечения. В данном случае сеть, которая подлежит сканированию, имеет адресное пространство 192.168.50.0/24.
Команда для выполнения данной задачи:
nmap -sP -sV 192.168.50.0/24
где -sP — включает режим пинг-сканирования, чтобы обнаружить все активные устройства в указанной сети, -sV — указывает на необходимость определения версий программного обеспечения для потенциального выявления уязвимостей.</td><td>nmap -sP -sV 192.168.50.0/24</td></tr>
</table>

	Этот подход обеспечит выявление активных устройств, а также поможет определить, какие из них могут использовать устаревшее или уязвимое ПО.	
Задание 10.	VLAN A: Маска /23 (512 IP-адресов, из которых 510 доступны для устройств) VLAN B: Маска /24 (256 IP-адресов, из которых 254 доступны для устройств) VLAN C: Маска /27 (32 IP-адреса, из которых 30 доступны для устройств) Общее количество IP-адресов: 512 + 256 + 32 = 800 IP-адресов.	**A:/23, B:/24, C:/27 Количество IP-адресов: 800**
Задание 11.	Для решения задачи нужно написать программу, которая будет вычислять хеш-значения для каждого пароля, используя предложенную формулу. Покажем решение по шагам и пример реализация кода программы на языке Python. **Шаги решения:** 1. Инициализируем значение начального вектора $H_0 = 5$. 2. Для каждого пароля последовательно вычисляем H_i на основе представленной формулы $H_i = (H_{i-1} + M_i)^2 mod\ 187$, где M_i — это позиция i-й буквы в алфавите. 3. После вычисления хеш-значения сравниваем его с заданным значением - 26. 4. Пароль, хеш которого совпадает с 26, будет ответом. **Пример программы на Python:**	**КРИПТОСТОЙКОСТЬ**

```
# Заданный алфавит и позиции букв
alphabet = {
   'А': 1, 'Б': 2, 'В': 3, 'Г': 4, 'Д': 5, 'Е': 6, 'Ё': 7, 'Ж': 8,
   'З': 9, 'И': 10, 'Й': 11, 'К': 12, 'Л': 13, 'М': 14, 'Н': 15, 'О': 16,
   'П': 17, 'Р': 18, 'С': 19, 'Т': 20, 'У': 21, 'Ф': 22, 'Х': 23, 'Ц': 24,
   'Ч': 25, 'Ш': 26, 'Щ': 27, 'Ъ': 28, 'Ы': 29, 'Ь': 30, 'Э': 31, 'Ю': 32, 'Я': 33
}

# Пароли для проверки
passwords = ["КОЛЛИЗИЯ", "ПРОКСИФИКАЦИЯ", "БЕЗОПАСНОСТЬ",
"АНАЛИТИК", "СИСТЕМА", "КРИПТОСТОЙКОСТЬ",
"АДМИНИСТРИРОВАНИЕ", "УПРАВЛЕНИЕ", "ПРЕОБРАЗОВАНИЕ",
"КЛАССИФИКАТОР"]

# Начальный вектор H0 и модуль n
H0 = 5
n = 187
correct_hash = 26

# Функция для вычисления хеша пароля
def calculate_hash(password):
   H = H0
```

		for letter in password:
		M_i = alphabet.get(letter, 0) # Получаем номер буквы в алфавите
		H = (H + M_i) ** 2 % n
		return H
		
		# Поиск пароля с правильным хешем
		for password in passwords:
		if calculate_hash(password) == correct_hash:
		print(f"Правильный пароль: {password}")
		break	

Приложение 5

Московский конкурс межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал»

Список учебной и методической литературы и другие источники

1. Шаньгин В.Ф. Информационная безопасность и защита информации / Шаньгин В.Ф. — 2-е изд. — Саратов: Профобразование, 2019. — 702 с.— 978-5-4488-0070-2.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети: Принципы, технологии, протоколы. Учебник. – СПб.: Питер, 2019. – 992 с.

3. Таненбаум Э.С., Фимстер Н., Уэзролл Д. Компьютерные сети. 6-е издание. – Санкт-Петербург: Питер, 2023. – 992 с.

4. Таненбаум Э., Бос Х., Современные операционные системы. / 4-е издание. Серия «Классика computer science». - СПб.: Питер. - 2015. – 1120 с. — ISBN 978-5-496-01395-6.