ИНТЕЛЛЕКТУАЛЬНЫЙ МЕГАПОЛИС

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

## ИТ-класс

в московской школе

## НАПРАВЛЕНИЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ТЕХНОЛОГИИ СВЯЗИ

## ПРАКТИЧЕСКИЙ ЭТАП

МОСКВА
2025

ИНТЕЛЛЕКТУАЛЬНЫЙ МЕГАПОЛИС

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ РАЗРАБОТАНЫ:

Подлесных Дмитрием Артуровичем - старшим преподавателем кафедры информатики и вычислительной техники МФТИ, тренером Центра развития ИТ-образования МФТИ.

МОСКВА
2025

# 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 *очной форме на базе вуза*. При выполнении работы обеспечивается строгое соблюдение порядка организации и проведения Конкурса.

*Дополнительные технические средства, разрешённые к использованию:* непрограммируемый калькулятор.

*Чем пользоваться категорически нельзя (ведет к отклонению работы):* веб-поиском.

## 3. Продолжительность выполнения

На выполнение всех заданий (6 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 *ответственного от вуза*. Мероприятие не продлевается на время отсутствия участника.

## 4. Содержание и структура

Индивидуальный вариант участника включает *6* заданий (задач), базирующихся на содержании *элективных курсов:* «Введение в ИТ-специальность» и «Информационные технологии». *В данном комплекте методических рекомендаций разбираются задания 4,5,6* индивидуального варианта участника.

## 5. Система оценивания

Задание считается выполненным, если ответ участника совпал с эталоном. Возможно выставление частичного балла в соответствии с критериями оценивания. Максимальный балл за выполнение совокупности заданий 4,5,6 – 30 баллов.

## 6. Приложения

1. План конкурсных материалов практического этапа Конкурса.
2. Демонстрационный вариант конкурсных заданий практического этапа Конкурса (задачи 4,5,6).
3. Критерии оценивания (задачи 4,5,6).
4. Примеры решения задач (задачи 4,5,6).
5. Список учебной и методической литературы, иные источники информации.

**Приложение 1.**
**План конкурсных материалов практического этапа Конкурса (задачи 4,5,6)**

| № задания | Уровень сложности | Уникальные кодификаторы Конкурса | Контролируемые требования к проверяемым умениям | Балл |
|---|---|---|---|---|
| 4 | *базовый* | 4.3.5. Методы и технологии защиты от вредоносных программ | Определять типы вредоносных программ.<br>Анализировать взаимодействие вредоносных программ с системой, состав выполняемых действий и используемых уязвимостей.<br>Оценивать потенциальные риски и последствия заражения вредоносным ПО для пользователей.<br>Уметь применять методы защиты от вредоносных программ. | 5 |
| 5 | *повышенный* | 4.1.3. Файловая система, интерфейс командной строки | Анализировать вывод стандартных утилит (интерпретация данных, мониторинг процессов, анализ системных журналов).<br>Анализировать состояние файловой системы (проверка целостности файлов, анализ прав доступа, мониторинг изменений в файловой системе).<br>Уметь применять меры защиты от атак. | 15 |
| 6 | *повышенный* | 4.1.6. Доменная система имен | Понимать структуру DNS.<br>Уметь взаимодействовать с записями DNS. | 10 |

| | | | | |
|---|---|---|---|---|
| | | | Владеть инструментами для анализа DNS.<br>Анализировать информацию из доменной системы имён.<br>Понимать принципы работы электронной почты.<br>Понимать структуру SPF записи. | |
| | | | | **Сумма баллов** | **30** |

**Приложение 2.**
**Демонстрационный вариант конкурсных заданий**
**практического этапа Конкурса (задачи 4,5,6)**

**Задача 4.**

Какая уязвимость позволяет удалённому атакующему выполнить произвольный код на стороне сервера? Допускается написание на русском или английском языках.

**Задача 5.**

В организации виртуальный сервер с 2 ядрами стал работать с перебоями.

Команда top вывела:

top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): **200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

| PID | USER | PR | NI | VIRT | RES | SHR | S | %CPU | %MEM | TIME+ | COMMAND |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1234 | vasya | 20 | 0 | 169652 | 14136 | 9084 | S | 200.0 | 20.0 | 1:44.60 | kswapd |
| 2 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.43 | kthreadd |
| 3 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | rcu_gp |
| 4 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | rcu_par+ |
| 5 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | slub_fl+ |
| 6 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | netns |
| 8 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | kworker+ |
| 10 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | mm_perc+ |
| 11 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | rcu_tas+ |
| 12 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | rcu_tas+ |
| 13 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | rcu_tas+ |
| 14 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:23.83 | ksoftir+ |
| 15 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 11:22.93 | rcu_pre+ |

**Задание:**

1. Определите, что произошло с сервером.
2. Укажите, что вызвало Ваши подозрения.
3. Какие меры нужно предпринять для ликвидации проблемы?
4. Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

**Задача 6.**

Пользователь vasya@itclass.su получил сообщение от владельцев сервера xmpp.jp с его аккаунтом. Вымогатель требует 120 ETH, угрожая опубликовать 100 500 кветтабайт переписки Васи, в которой он обсуждает действия, описываемые главой 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной безопасности».

```
Received: from relay1.ele-ele.com (91.215.42.222)
      by relay1.telecom.mipt.ru (Postfix) with SMTP id 29467120A4F
      for <vasya@itclass.su>; Tue, 30 Apr 2025 18:26:20 +0300 (MSK)
Message-Id: <202504130152728.01AA81207D9@relay1.ele-ele.com>
Date: Tue, 30 Apr 2025 18:27:28 +0300 (MSK)
From: interpol@xmpp.jp

;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44221
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xmpp.jp.                IN      TXT

;; ANSWER SECTION:
xmpp.jp.          300   IN      TXT     "v=spf1 ip4:153.121.46.102 ip4:133.125.47.57
~all"

;; AUTHORITY SECTION:
xmpp.jp.          7200  IN      NS      arya.ns.cloudflare.com.
xmpp.jp.          7200  IN      NS      clay.ns.cloudflare.com.

;; ADDITIONAL SECTION:
arya.ns.cloudflare.com. 4785    IN      A       173.245.58.70
arya.ns.cloudflare.com. 4785    IN      A       108.162.192.70
```

```
arya.ns.cloudflare.com. 4785    IN      A       172.64.32.70
clay.ns.cloudflare.com. 5462    IN      A       172.64.33.88
clay.ns.cloudflare.com. 5462    IN      A       173.245.59.88
clay.ns.cloudflare.com. 5462    IN      A       108.162.193.88
clay.ns.cloudflare.com. 5772    IN      AAAA    2803:f800:50::6ca2:c158
clay.ns.cloudflare.com. 5772    IN      AAAA    2a06:98c1:50::ac40:2158
clay.ns.cloudflare.com. 5772    IN      AAAA    2606:4700:58::adf5:3b58

;; Query time: 0 msec
;; SERVER: 10.21.50.10#53(10.21.50.10)
;; WHEN: Wed May 07 11:01:18 MSK 2025
;; MSG SIZE  rcvd: 332
```

**Задание:**

Можно ли доверять вымогателю? Ответ обоснуйте на основе анализа объёма информации и адреса отправителя.

**Приложение 3.**
**Критерии оценивания (задачи 4,5,6)**

**Задача 4.**

**Критерии оценивания:**

Максимальное количество баллов за задание – 5.

| | |
|---|---|
| Учащийся дал точный и корректный ответ (без орфографических ошибок, в верхнем или нижнем регистре допустимо: RCE, remote code execution, удаленное исполнение кода) | 5 |
| Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка | 3 |
| Ответ неправильный, либо отсутствует | 0 |

**Задача 5.**

**Критерии оценивания:**

Максимальное количество баллов за задание – 15.

| | | |
|---|---|---|
| **Расследование** | | **3** |
| Учащийся правильно определяет, что kswapd должен быть запущен от root’а, запуск от пользователя vasya указывает на подделку | 1 | |
| Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap | 1 | |
| Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером | 1 | |
| **Меры по ликвидации проблемы** | | **7** |
| Убит процесс | 1 | |
| Вредоносный исполняемый файл найден и переименован для дальнейшего анализа | 1 | |
| У вредоносного исполняемого файла удалены права на исполнение | 1 | |
| Заблокирован вход пользователю vasya по паролю | 1 | |
| Удалены авторизованные ключи пользователя vasya | 1 | |
| Удалены задачи пользователя vasya в crontab | 1 | |
| Проверены задачи других пользователей | 1 | |
| **Меры по предотвращению проблемы** | | **5** |
| Разрешён вход по ssh только по ключам | 1 | |
| Вход по ssh разрешён только из рабочей сети (или VPN в неё) | 1 | |
| Скомпрометированная система восстановлена из резервной копии | 1 | |
| Сервисы помещены в контейнеры с ограничением ресурсов | 1 | |
| У пользователей ограничены ресурсы | 1 | |
| **ИТОГО** | | **15** |

**Задача 6.**

**Критерии оценивания:**

Максимальное количество баллов за задание – 10.

| | |
|---|---|
| Объём информации нереалистичен | **5** |
| Адреса отправителя не соответствует SFP записи | **5** |
| **ИТОГО** | **10** |

**Приложение 4.**
**Примеры решения задач (задачи 4,5,6)**

**Задача 4.**

Ответ: remote code execution, сокращённо RCE.

**Задача 5.**

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (2 ядра из 2 имеющихся) наводит на мысль, что это – майнер.

Найдём, что это за исполняемый файл (ls -al */proc/1234/executable),* убьём процесс (kill -9 1234), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.

Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/autorized_keys /tmp/vasya_kswapd_keys*, *rm /home/vasya/.ssh/autorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).

Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

**Задача 6.**

1. 100500 * $10^{30}$ байтов — нереалистичный объём информации.

2. IP 91.215.42.222 не соответствует spf1-записи для xmpp.jp

ip4:153.121.46.102 ip4:133.125.47.57 ~all

**Приложение 5.**
**Список учебной и методической литературы, иные источники информации**

1. Миронов В.Н. Основы информационной безопасности: Учебник для среднего профессионального образования. — М.: Издательство Юрайт, 2023.— ISBN 978-5-534-13885-7.
2.Скляров Д.В. Искусство защиты информации. — СПб.: БХВ-Петербург, 2006. — 464 с. - ISBN 5-94157-963-8.
2. Энциклопедия кибербезопасности. Под ред. А.В. Петренко. - М.: Горячая линия - Телеком, 2018. - 416 с.
3. Джейсон Шэтц. Руководство по информационной безопасности для начинающих. – М.: Эксмо, 2023. - ISBN: 978-5-04-170689-1.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети: Принципы, технологии, протоколы. Учебник. – СПб.: Питер, 2019. – 992 с.

**Иные источники информации (интернет-ресурсы):**

1. Positive Technologies https://ptsecurity.com/ru-ru/research/
2. Kaspersky Daily https://www.kaspersky.ru/blog/
3. Hacktricks https://book.hacktricks.wiki/en/index.html
5. Root-me https://www.root-me.org/?lang=en
6. picoCTF https://picoctf.org/