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.

Дополнительное оборудование, разрешённое для прохождения: непрограммируемый калькулятор

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

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 *ответственного от вуза*. Мероприятие не продлевается на время отсутствия участника.

4. Содержание и структура

Индивидуальный вариант участника включает *6* заданий, базирующихся на содержании *элективных курсов: «Введение в ИТ-специальность» и «Информационные технологии».*

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 всех заданий – 60 баллов.

6. Приложения

1. План конкурсных материалов для проведения практического этапа Конкурса.
2. Демонстрационный вариант конкурсных заданий практического этапа Конкурса.
3. Критерии оценивания
4. Пример решения задач.

Приложение 1

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.	-	базовые	*IP-адресация. Доменная система имён. Расчет количества компьютеров в сети*	Выполнять расчёт необходимого количества IP-адресов в подсети с учётом количества конечных устройств, планируемого прироста и резервирования адресного пространства для служебных целей (сетевой адрес и широковещательный адрес). Определять минимально допустимый префикс подсети (CIDR), исходя из рассчитанного количества адресов, и обосновывать выбор на основе двоичной структуры адресации. Оценивать возможности адресного пространства базовой сети, рассчитывая количество возможных подсетей заданного размера, и делать вывод о достаточности или недостаточности ресурса IP-адресов. Формировать корректные доменные имена в соответствии с заданным шаблоном, отражающим иерархию внутриорганизационной сети, и анализировать структуру DNS-имени по уровням (имя хоста, поддомен, домен организации, домен верхнего уровня)	12
2	-	базовый	*История Интернета.*	Описывать ключевые этапы развития Интернета, включая	3

			Организация обмена информацией. Применяемые типы шифрования (HTTPS)	создание ARPANET, внедрение протокола TCP/IP и развитие Всемирной паутины. Понимать архитектуру взаимодействия узлов в Интернете, принципы маршрутизации и модели клиент-серверного обмена данными. Объяснять принципы безопасного соединения по протоколу HTTPS: использование TLS/SSL, роль сертификатов и центра сертификации (CA), установление защищённого канала. Идентифицировать используемые алгоритмы шифрования в HTTPS-соединениях, различать симметричное и асимметричное шифрование и понимать их совместное применение при установлении соединения. Оценивать значение безопасности передаваемой информации, анализировать угрозы при передаче данных по открытым каналам связи и способы их минимизации	
3	-	повышенный	*Алгоритмы шифрования (RSA). Основы хеширования. Хеш-функции*	Выполнять базовые вычисления в алгоритме RSA: Вычисление модуля n, функции Эйлера \varphi(n), нахождение закрытого ключа d по открытому ключу e. Применять степенной модуль для формирования цифровой подписи: умение использовать формулу s = H^d \mod n. Понимать принципы работы цифровой подписи: связь между хешированием,	15

				шифрованием и проверкой подлинности сообщения.	
4	-	базовый	*Возможности вредоносных программ*	Определять типы вредоносных программ. Анализировать взаимодействие вредоносных программ с системой, состав выполняемых действий и используемых уязвимостей. Оценивать потенциальные риски и последствия заражения вредоносным ПО для пользователей. Уметь применять методы защиты от вредоносных программ.	5
5	-	повышенный	*Файловая система, интерфейс командной строки*	Анализировать вывод стандартных утилит (интерпретация данных, мониторинг процессов, анализ системных журналов). Анализировать состояние файловой системы (проверка целостности файлов, анализ прав доступа, мониторинг изменений в файловой системе). Уметь применять меры защиты от атак.	15
6	-	повышенный	*Доменная система имён*	Понимать структуру DNS. Уметь взаимодействовать с записями DNS. Владеть инструментами для анализа DNS. Анализировать информацию из доменной системы имён. Понимать принципы работы электронной почты. Понимать структуру SPF записи.	10
				Сумма баллов:	**60**

ИНТЕЛЛЕКТУАЛЬНЫЙ МЕГАПОЛИС

Приложение 2

Демонстрационный вариант №1 конкурсных заданий *практического* этапа Конкурса

Задача 1.

В организации используется частная IP-сеть с адресом **192.168.10.0/24**. Необходимо организовать отдельную подсеть для одного отдела, в котором сейчас работает **30 человек**, и планируется увеличить количество рабочих устройств на 20% в ближайшее время.

Каждому компьютеру в отделе должно быть назначено уникальное доменное имя вида **hostX.department.company.local**, где X — **номер компьютера**.

Задание:

1. Определите, какой наименьший префикс подсети (CIDR) нужно использовать для этого отдела, чтобы удовлетворить текущие и будущие потребности.
2. Рассчитайте, сколько таких подсетей можно создать из 192.168.10.0/24.
3. Приведите пример полного доменного имени одного компьютера и кратко поясните, из каких уровней оно состоит.

Критерии оценивания:

Максимальная количество баллов за задание – 12.

Расчет необходимого количества IP-адресов		**3**
учащийся правильно определяет количество устройств, учитывает служебные IP-адреса (broadcast и network), делает вывод	3	
прирост учтён, служебные адреса не учтены	2	
рассчитано число устройств без прироста или с ошибкой округления	1	
расчет не выполнен или выполнен неправильно, не учтён прирост или приведено случайное число	0	
Определение минимального подходящего префикса подсети (CIDR)		**3**
правильно выбран префикс, с обоснованием хоста	3	
выбран подходящий префикс, но расчёт не учитывает служебные адреса	2	
выбран верный диапазон, но неверный префикс (например, /25, что даёт избыточные 126 хостов) или отсутствует обоснование	1	
префикс выбран неверно (например, /27 или /30), не соответствует потребностям, нет расчёта	0	
Расчёт количества возможных подсетей с выбранным префиксом		**3**
верно вычислено, показан расчёт	3	
подсетей указано верное количество, но без пояснений или с ошибкой в делении	1	
неверный ответ (например, 2 или 8), отсутствует логика вычислений	0	
Пример доменного имени и объяснение структуры DNS		**3**
дан корректный пример (например, host5.it.company.local) и правильно объяснены все 4 уровня: хост → поддомен → домен → TLD	3	
имя указано верно, но структура описана неполно (например, не упомянут уровень хоста или поддомена)	1	

имя не соответствует формату задачи или структура домена не описана вообще / с грубыми ошибками	0	
ИТОГО		**12**

Задача 2.

Какой рекомендованный на сегодняшний день протокол используется для безопасной передачи данных в Интернете и сочетает симметричное и асимметричное шифрование? Укажите полное название протокола.

Критерии оценивания:

Максимальная количество баллов за задание – 3.

Ученик дал точный и корректный ответ (без орфографических ошибок, в верхнем или нижнем регистре допустимо: https, HTTPS).	3
Ответ близкий по смыслу, но частично некорректный (например, допущена незначительная орфографическая ошибка)	1
Ответ неправильный, либо отсутствует	0

Задача 3.

Вам нужно подписать сообщение с использованием упрощённого алгоритма RSA и передать только его цифровую подпись. Для создания ключей выбраны простые числа p = 17 и q = 11. В качестве открытой экспоненты используется e = 7. Хеш-сумма сообщения вычислена заранее и составляет 9.

Какое значение будет иметь цифровая подпись этого сообщения?

Ответом должно быть одно число — значение цифровой подписи.

Подписью считается результат возведения хеш-суммы в степень d *по модулю* n.

Все промежуточные вычисления делаются самостоятельно, но в ответе требуется только значение подписи.

Критерии оценивания:

Максимальная количество баллов за задание – 15.

Ученик дал **корректный финальный ответ** и при проверке показал **все основные этапы вычислений**: правильно найдено n, \varphi(n), d, и вычислена цифровая подпись по формуле s = H^d \mod n. Все этапы выполнены без ошибок.	15
Финальный ответ верный или содержит незначительную вычислительную ошибку (например, ошибка в модуле, но логика верная). Показаны почти все ключевые шаги, возможно, с одной арифметической неточностью. Понимание RSA подтверждено.	12
Финальный ответ неверный, но ученик верно выполнил **часть ключевых этапов** (например, нашёл n и \varphi(n), но ошибся при нахождении d или при возведении в степень). Общая логика RSA прослеживается.	8

Ученик правильно выполнил хотя бы один ключевой шаг (например, нашёл n), продемонстрировал общее понимание задачи, но допустил грубые ошибки в модульной арифметике или неправильно применил формулы.	4
Есть попытка подставить числа или назвать формулы, но они не соответствуют RSA. Понимание темы минимально. Пример: $H \cdot e \ mod \ n$ вместо $H^d \ mod \ n$.	1
Ответ отсутствует, бессвязный, или ученик не приступал к решению.	0

Задача 4.

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

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.

В организации виртуальный сервер с двумя 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?

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.

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.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

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

Пример решения заданий практического этапа Конкурса.

Задача 1.

1. Кол-во устройств: $30 \cdot (20\% + 100\%) = 36$ - минимальное количество IP-адресов для хостов.
2. При использовании IPv4 с учетом сетевого и широковещательного адресов, общее количество адресов в подсети - 38.
   a. Префикс /26: Количество адресов - 64, количество хостов 62
   b. Префикс /27: Количество адресов - 32, количество хостов 30

Таким образом, минимальный префикс - /26

3. /24 - содержит 256 IP-адресов, тогда из 192.168.10.0/24 можно создать: $\frac{256}{64} = 4$ подсети /26.
4. Например, для хоста №5: **host5.department.company.local**

Уровни в доменном имени:

- **host5** — имя конкретного устройства (хост).
- **department** — поддомен, указывающий на отдел в организации.
- **company** — домен организации.
- **local** — верхнеуровневый домен (обычно используется в локальных сетях).

Задача 2.

Ответ: Протокол, в котором применяется и симметричное, и асимметричное шифрование для безопасной передачи данных в Интернете — это TLS (Transport Layer Security).

Задача 3.

1. $n = p \times q = 17 \times 11 = 187$
2. $\varphi(n) = (p-1)(q-1) = 160$
3. $d = e^{-1} \, mod \, \varphi(n) = 23$
4. $S = H^d \, mod \, n = 9^{23} \, mod \, 187$

$$9^2 = 81 \; mod \; 187 = 81$$
$$9^3 = 729 \, mod \; 187 = 168$$
$$9^4 = 6561 \, mod \; 187 = 16$$
$$9^5 = 59049 \, mod \; 187 = 144$$

5. $S = H^d \, mod \, n = 9^{23} \, mod \, 187 = 9^3 * 9^{20} \, mod \, 187 = 9^3 * (9^{10})^2 \, mod \, 187 = = 168 * ((144)^2)^2 \, mod \, 187 = 168 * (20736)^2 \, mod \, 187 = 168 * 166^2 \, mod \, 187 =$

$$= 168 * 67 \, mod \, 187 = 11256 \, mod \, 187 = 36$$

Ответ: 36

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

Демонстрационный вариант №2 конкурсных заданий *практического* этапа Конкурса

Задача 1.

В компании используется частная IP-сеть с адресом **10.0.0.0/24**. Необходимо организовать отдельную подсеть для отдела разработки, в котором сейчас работает **45 человек**, и планируется увеличение количества рабочих устройств на **25%** в течение года.

Каждому устройству должен быть присвоен уникальный доменный адрес формата **devX.dev.company.local**, где **X — номер устройства**.

Задание:

1. Определите, какой наименьший префикс подсети (CIDR) нужно использовать для отдела разработки, чтобы удовлетворить текущие и будущие потребности.
2. Рассчитайте, сколько таких подсетей можно создать из сети **10.0.0.0/24**.
3. Приведите пример одного полного доменного имени и кратко поясните структуру его уровней

Критерии оценивания:

Максимальная количество баллов за задание – 12.

Расчет необходимого количества IP-адресов		**3**
учащийся правильно определяет количество устройств, учитывает служебные IP-адреса (broadcast и network), делает вывод	3	
прирост учтён, служебные адреса не учтены	2	
рассчитано число устройств без прироста или с ошибкой округления	1	
расчет не выполнен или выполнен неправильно, не учтён прирост или приведено случайное число	0	
Определение минимального подходящего префикса подсети (CIDR)		**3**
правильно выбран префикс, с обоснованием хоста	3	
выбран подходящий префикс, но расчёт не учитывает служебные адреса	2	
выбран верный диапазон, но неверный префикс (например, /25, что даёт избыточные 126 хостов) или отсутствует обоснование	1	
префикс выбран неверно (например, /27 или /30), не соответствует потребностям, нет расчёта	0	
Расчёт количества возможных подсетей с выбранным префиксом		**3**
верно вычислено, показан расчёт	3	
подсетей указано верное количество, но без пояснений или с ошибкой в делении	1	
неверный ответ (например, 2 или 8), отсутствует логика вычислений	0	
Пример доменного имени и объяснение структуры DNS		**3**
дан корректный пример (например, host5.it.company.local) и правильно объяснены все 4 уровня: хост → поддомен → домен → TLD	3	
имя указано верно, но структура описана неполно (например, не упомянут уровень хоста или поддомена)	1	
имя не соответствует формату задачи или структура домена не описана вообще / с грубыми ошибками	0	
ИТОГО		**12**

Задача 2.

На каком уровне модели OSI работает протокол IP (Internet Protocol), который отвечает за маршрутизацию и доставку пакетов между сетями?

Укажите название уровня модели OSI.

Критерии оценивания:

Максимальная количество баллов за задание – 3.

Ученик дал точный и корректный ответ (без орфографических ошибок, в верхнем или нижнем регистре допустимо: https, HTTPS).	3
Ответ близкий по смыслу, но частично некорректный (например, допущена незначительная орфографическая ошибка)	1
Ответ неправильный, либо отсутствует	0

Задача 3.

Вы получили цифровую подпись сообщения, выполненную с помощью упрощённого алгоритма RSA. Теперь необходимо проверить подлинность этой подписи.

Открытый ключ отправителя содержит числа:

- n = 143
- e = 7

Цифровая подпись, полученная вместе с сообщением, равна **125**.

Хеш-сумма переданного сообщения, вычисленная получателем самостоятельно, составляет **5**. Если результат совпадает с хеш-суммой, подпись считается подлинной.

Ответом должно быть слово «да» или «нет» — в зависимости от того, подтверждает ли подпись подлинность сообщения.

Для проверки подлинности необходимо возвести цифровую подпись в степень e по модулю n и сравнить результат с хеш-суммой.

Все промежуточные вычисления делаются самостоятельно, но в ответе требуется только слово «да» или «нет».

Критерии оценивания:

Максимальная количество баллов за задание – 15.

Ученик дал **верный финальный ответ (“да” или “нет”)** и корректно выполнил **все ключевые этапы вычислений**: возведение подписи в степень e, нахождение результата по модулю n, сравнение с хешем. Все шаги оформлены ясно, ошибок в логике или арифметике нет.	5
Финальный ответ **верный** или содержит **незначительную арифметическую ошибку**, не влияющую на общее понимание процесса (например, ошибка в последнем действии модуля). Основные шаги вычислений показаны, логика RSA корректно прослеживается.	2

Финальный ответ **неверный**, но ученик **правильно выполнил часть ключевых действий** (например, возведение в степень выполнено верно, но ошибка в модуле или не сравнил с хешем). Общая идея проверки RSA-подписи понятна.	8
Ученик показал **хотя бы один значимый шаг** (например, попытался возвести в степень или применить модуль), но остальная часть решения содержит серьёзные ошибки. Понимание алгоритма поверхностное, но попытка есть.	4
Имеется **формальная попытка** решения: подставлены числа или названы формулы, но они **не соответствуют сути RSA**. Например, перепутаны роли ключей или неверно применены формулы (например, H^e \mod n, когда нужно s^e \mod n).	1
Ответ отсутствует, бессвязный, либо ученик дал верный или неверный ответ, но не приступал к решению задания (не показал никаких вычислений или логики).	0

Задача 4.

Какая уязвимость позволяет пользователю web-сайта выполнить произвольный запрос к базе данных? Допускается написание на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ (без орфографических ошибок, в верхнем или нижнем регистре допустимо: SQL-инъекция, sql injection)	5
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	3
Ответ неправильный, либо отсутствует	0

Задача 5.

В организации виртуальный сервер с 100-гигабайтным жёстким диском стал работать с перебоями.

Команда df вывела:

```
root@server#df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           3.9G  4.0K  3.9G   1% /dev/shm
tmpfs           1.6G  9.7M  1.6G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/sda7        95G   95G   0G  100% /
tmpfs           795M     0  795M   0% /run/user/0
```

Команда mount вывела:

```
root@server# mount| grep sd
/dev/sda7 on / type ext4 (rw,relatime)
```

Команда du -h -s /home/*/*| grep G вывела:

root@server# du -h -s /*home*/*/* | grep G

80G /*home/vasya/PoS*

Задание:

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

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определил, что кончилось дисковое пространство	1	
Учащийся определил, что из разделов жёстких дисков смонтирован только sda7	1	
Учащийся определил, что PoS, полностью использующий дисковое пространство, может быть майнером криптовалюты по принципу Proof-of-Storage	1	
Меры по ликвидации проблемы		**7**
Использован резерв суперпользователя tune2fs -m 0 /*dev*/sda7	1	
Смонтирован накопитель для резервного копирования	1	
Каталог PoS перемещён на резервный накопитель	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.

Пользователю vasya@itclass.su пришло письмо с весьма заманчивым предложением о работе с зарплатой в размере 100 500 биткоинов в наносекунду. Согласно тексту письма, на работу приглашает сам президент США.

Received: from relay1.ele-ele.com (91.215.42.222)
by relay2.ele-ele.com (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: president@whitehouse.gov

Вася стал исследовать:

dig TXT whitehouse.gov

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> TXT whitehouse.gov
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48355
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4e273de0d13e9dcf01000000681b09d7758699a04cb83116 (good)
;; QUESTION SECTION:
;whitehouse.gov. IN TXT

;; ANSWER SECTION:
whitehouse.gov. 3600 IN TXT "_ag15rep8dkdk6c65mcqgkcmtszqxbqt"
whitehouse.gov. 3600 IN TXT "v=spf1 include:spf.mail.dmz.pitc.gov include:spf.mandrillapp.com ip4:214.3.115.10/32 ip4:214.3.115.12/32 ip4 :214.3.115.14/32 ip4:214.3.115.225/32 ip4:214.3.140.16/32 ip4:214.3.140.22/32 ip4:214.3.140.255/32 ~all"
whitehouse.gov. 3600 IN TXT "google-site-verification=TfE8QdIcAwpNcoG9l9AxMIzz69S5PPd8peS-Pj1qtXk"

;; Query time: 8 msec
;; SERVER: 81.5.91.3#53(81.5.91.3) (UDP)
;; WHEN: Wed May 07 10:20:55 MSK 2025
;; MSG SIZE rcvd: 421

Задание:

Можно ли доверять отправителю? Ответ обоснуйте на основе приведённых данных по биткоинам в связанности с наносекундами и информации в части адреса отправителя.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Всего может быть 21 миллион биткоинов, зарплата за 209 наносекунд	5
Адреса отправителя не соответствует SFP записи	5

ИТОГО	10

Пример решения заданий практического этапа Конкурса.

Задача 1.

1. Кол-во устройств: $45 \cdot (25\% + 100\%) = 57$ - минимальное количество IP-адресов для хостов.
2. При использовании IPv4 с учетом сетевого и широковещательного адресов, общее количество адресов в подсети - 59.

a. Префикс /26: Количество адресов - 64, количество хостов 62

b. Префикс /27: Количество адресов - 32, количество хостов 30

Таким образом, минимальный префикс - /26

3. /24 - содержит 256 IP-адресов, тогда из 192.168.10.0/24 можно создать: $\frac{256}{64} = 4$ подсети /26.
4. Например, для хоста №7: **dev7.dev.company.local**

Уровни в доменном имени:

- **dev7** — имя хоста (устройства)
- **dev** — поддомен, обозначающий отдел разработки
- **company** — домен организации
- **local** — верхнеуровневый домен, указывающий на локальную сеть
-

Задача 2.

Ответ: IP-протокол работает на сетевом уровне модели OSI.

Задача 3.

1. $n = 143$
2. $125^7 mod\ 143\ ? = 5$

$$7 = 1 + 2 + 4$$

$$125^2\ mod\ 143 = 38$$

$$125^4\ mod\ 143 = 14$$

$$125^7\ mod\ 143 = 125^1 * 125^2 * 125^4 = 125 * 38 * 14\ mod\ 143 = 5$$

Ответ: Да

Задача 4.

Ответ: SQL-инъекция.

Задача 5.

Видим, что закончилось место на 100-гигабайтном жёстком диске, но видим только 95 Гб на файловой системе ext4. Значит, есть стандартные 5 Гб, зарезервированные для суперпользователя. По занятому месту видим, что дисковое пространство потребляет пользователь vasya, причём в каталоге PoS. Это сразу наводит на подозрения, что это – майнер на базе предоставления жёсткого диска как места хранения.

Чтобы система была управляемой, разблокируем зарезервированные 5%.

tune2s -m 0 /dev/sda7

Смонтируем резервный накопитель, перенесём на него PoS, поинтересуемся у Васи, с какой целью он майнит криптовалюту на рабочем сервере и предупредим об ответственности.

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. Всего может быть 21 миллион биткоинов. При зарплате 100 500 биткоинов в наносекунду они исчерпаются за 209 наносекунд.

2. Адреса отправителя не соответствует SPF записи домена whitehouse.gov.