ИНТЕЛЛЕКТУАЛЬНЫЙ МЕГАПОЛИС

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ИТ-класс

в московской школе

НАПРАВЛЕНИЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ТЕХНОЛОГИИ СВЯЗИ

ПРАКТИЧЕСКИЙ ЭТАП

МОСКВА
2025

ИНТЕЛЛЕКТУАЛЬНЫЙ МЕГАПОЛИС

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ РАЗРАБОТАНЫ:

Евдокимова Екатерина Александровна, заместитель начальника организационно-методического отдела УПРА РТУ МИРЭА

МОСКВА
2025

Методические рекомендации для учащихся предпрофессиональных классов

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

Москва
2025

Содержание

Рекомендации к выполнению конкурсных вариантов

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

Во время практического этапа участникам **строго запрещено** пользоваться веб-поиском; из технических средств допускается только **непрограммируемый калькулятор** . Все задания рассчитаны на самостоятельное решение с базовыми вычислениями вручную или на калькуляторе. Ниже приведены рекомендации по ключевым тематическим блокам заданий – они охватывают знания и умения, необходимые учащимся 10–11 классов для успешного выполнения каждого вида задач, включая IP-адресацию, DNS, модель OSI, HTTPS и RSA.

1. IP-адресация и доменные имена

Участник должен знать двоичную структуру IPv4-адресов и уметь определять минимально допустимый префикс (CIDR) для заданного количества хостов с учётом резервирования адресов для сетевого и широковещательного назначения. Расчёт выполняется по формуле: , где — число хостов, — служебные адреса. Для определения количества возможных подсетей необходимо использовать формулу: , где — префикс базовой сети, — найденный префикс подсети.

В вопросах по DNS-адресации важно разложить имя по уровням, начиная с имени хоста и заканчивая доменом верхнего уровня. Рекомендуется приводить пример имени и пояснять его структуру

2. Безопасность интернет-соединений

Требуется знать названия и функции всех семи уровней модели OSI. Для каждого указанного протокола необходимо уметь определить, к какому уровню он относится. Для этого полезно запомнить сопоставление: IP — L3, TCP/UDP — L4, HTTP — L7 и т.д. При решении задачи рекомендуется по ключевому действию протокола (доставка, маршрутизация, соединение и др.) определить его функциональный уровень.

Участник должен знать хронологию ключевых событий: ARPANET, переход к TCP/IP (1983), развитие модели клиент-сервер. Для решения задач по этой теме полезно

опираться на таблицу соответствий протоколов и их задач (например, DHCP — автоматическая настройка IP, DNS — преобразование имён в адреса). При сравнении IPv4 и IPv6 следует указывать битность, структуру, объём адресного пространства.

Для выполнения заданий требуется чётко различать симметричное и асимметричное шифрование. На этапе TLS-handshake происходит обмен ключами с использованием RSA или аналогичных алгоритмов, после чего устанавливается симметричный алгоритм (AES и др.). При ответе на вопросы рекомендуется перечислять этапы установления HTTPS-соединения. Также важно знать, какие поля содержатся в сертификате и чем отличается сертификат, подписанный центром сертификации (CA), от самоподписанного. При описании механизмов проверки отзыва сертификата необходимо указывать OCSP и CRL как альтернативные подходы.

3. RSA и цифровая подпись

Для успешного выполнения задач по RSA участник должен владеть приёмами вычисления по модулю. Задачи могут быть на создание или проверку подписи. В первом случае требуется:

Найти $\mathrm{n} = \mathrm{p} \times \mathrm{q}$;

Вычислить $\varphi(n) = (p-1)(q-1)$;

Убедиться, что e взаимно просто с $\varphi(\mathrm{n})$;

Найти как обратное к по модулю $\varphi(\mathrm{n})$;;

Вычислить подпись $s = H^d \ mod \ n$: .

Для проверки подписи: $s^e mod \ n = ? H$. Все вычисления должны сопровождаться пояснениями. Для упрощения можно использовать метод последовательного возведения в степень с промежуточным модулем.

Демонстрационный вариант 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:

Определите, какой наименьший префикс подсети (CIDR) нужно использовать для этого отдела, чтобы удовлетворить текущие и будущие потребности. Затем рассчитайте, сколько таких подсетей можно создать из 192.168.10.0/24. 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

Список литературы для подготовки

1. Харитонов А., Джаманкулов А. КОМПЬЮТЕРНЫЕ СЕТИ И ПРОТОКОЛЫ ПЕРЕДАЧИ ДАННЫХ.
2. Баринов В. В., Баринов И. В., Пролетарский А. В. Компьютерные сети: Учебник //М.: Academia. – 2018. – Т. 192.
3. Горбатов В. С., Полянская О. Ю. Основы технологии PKI. – 2011.
4. Келдыш Н. В. Системная защита информации компьютерных сетей. – 2022.
5. Венедюхин А. Как работает TLS, в технических подробностях / Венедюхин А. [Электронный ресурс] // TLS : [сайт]. — URL: https://tls.dxdt.ru/tls.html