Задания для муниципального этапа всероссийской олимпиады школьников по информатике и ИКТ, профиль «Информационной безопасности» для 9-11 классов, 2025/26 уч.год.

МАКСИМАЛЬНОЕ КОЛИЧЕСТВО БАЛЛОВ— 200 БАЛЛОВ.
ВРЕМЯ ВЫПОЛНЕНИЯ: 180 МИНУТ.

Задание 1.

Клиент крупного банка, Владимир, собрался оплатить кредит через онлайн-банк. Он, как всегда, набрал в браузере «mybank.ru» и нажал «Enter.» Однако злоумышленник подменил IP-адрес легитимного сервера в DNS-ответе, направив пользователя на фальшивый сайт. Как называется такая атака?

Ответ: DNS-спуфинг (или DNS-кэширование).

Пояснение: DNS-спуфинг — это кибератака, при которой злоумышленник подменяет соответствие между доменным именем и IP-адресом, чтобы перенаправить пользователя на фальшивый (часто вредоносный сайт).

Критерии оценивания: за правильный ответ — 2 балла.

Задание 2.

Операция «Тайный майнер: расследование компрометации сервера».

Вы — член команды SOC (Security Operations Center) компании *DataSafe*. В 14:30 по местному времени система мониторинга *SIEM* выдала серию «алертов» по ключевому серверу.

На сервере:

-резко вырос исходящий трафик;

-в процессах виден неизвестный процесс miner;

-в cron добавлены задания с подозрительными URL.

1. Опишите, что произошло?

2.Перечислите три шага по реагированию на инцидент информационной безопасности.

Ответ:

1. Сервер заражён вредоносным ПО (miner).

2. Шаги:

-изолировать сервер от сети;
-собрать лог-файлы и дампы памяти;
-удалить вредоносные процессы и задания cron;
-сменить пароли и ключи;
-обновить ПО и закрыть уязвимости.

Критерии оценивания: за каждый правильный ответ — 1 балл.
Всего за это задание можно получить 5 баллов.

Задание 3.

Ответье на вопрос, какой файл в Linux хранит хеши паролей пользователей?
1./etc/passwd
2./etc/shadow
3./etc/group
4./etc/hosts

Ответ: 2.
Пояснение: /etc/shadow содержит хеши паролей и параметры их смены (доступен только root).

Критерии оценивания: за правильный ответ — 3 балла.

Задание 4.

Ответьте на вопрос**,** для чего используется стандарт **LUKS** в Linux?
1. Шифрование разделов диска.
2. Сжатие файлов.
3.Резервное копирование в облако.
4.Ускорение работы SSD.

Ответ: 1.
Пояснение: LUKS (Linux Unified Key Setup) — стандарт шифрования дисков/разделов.
Критерии оценивания: за правильный ответ — 3 балла.

Задание 5.

В логах сервера множество http-запросов с разными User-Agent, но одним IP-адресом. Каждый запрос содержит параметр ?id=1' OR '1'='1. Что это?

1.DDoS-атака.
2.Попытка SQL-инъекции.
3.Сканирование портов.
4.Фишинговая рассылка.

Ответ: 2.
Пояснение: строка `1' OR '1'='1` — классический пример SQL-инъекции.

Критерии оценивания: за правильный ответ — 2 балла.

Задание 6.

Администратор сети выполняет в терминале Linux следующую команду:
`ping -c 5 -i 2 -W 3 mail.ru`

Опишите пошагово, что произойдёт при выполнении этой команды, и объясните значение каждой опции. Ответьте, какой вывод можно сделать по итоговой статистике, если получено 3 ответа из 5, среднее время отклика — 45 мс, а максимальное — 120 мс?

Требования к ответу:
1.Раскройте смысл каждой опции команды (`-c`, `-i`, `-W`).
2.Опишите последовательность действий утилиты `ping` при выполнении команды.
3.Проанализируйте приведённую статистику:
-что означает 3 ответа из 5?
-о чём говорит разброс времени отклика (45 мс vs 120 мс)?
-какие возможные причины таких результатов?

Пример правильного ответа:
1.Опции:
•`-c 5` — отправить ровно 5 пакетов.
•`-i 2` — интервал между пакетами 2 секунды.
•`-W 3` — ждать ответа на каждый пакет не более 3 секунд.
2.Процесс: отправка 5 пакетов с интервалом 2 с; на каждый ответ ожидается до 3 с; по итогам — сводка статистики.
3.Анализ:
3/5 — 40 % потерь, возможная нестабильность связи.
Разброс времени (45→120 мс) — перегрузки на маршруте или колебания загрузки сети.

Критерии оценивания:
Точность объяснения опций команды (максимально - 3 балла).
Корректность описания процесса выполнения (максимально - 2 балла).
Глубина анализа статистики и причин (максимально - 4 балла).

Всего за это задание можно получить 9 баллов.

Задание 7.

Злоумышленник использует анализатор сетевого трафика Wireshark в сети с общим хабом (hub). Что он может получить?
1.Все пакеты, проходящие через хаб.
2.Только пакеты, адресованные его MAC.
3.Ничего — трафик зашифрован.

Ответ: 1.
Пояснение: хаб рассылает все пакеты на все порты; в отличие от коммутатора (switch), нет изоляции трафика.

Критерии оценивания: за правильный ответ — 2 балла.

Задание 8.

Вы — специалист группы реагирования на инциденты в компании *SecureTech*. Вам поступил тревожный сигнал: в течение последних 2 часов наблюдаются аномалии в работе корпоративной сети.

Исходные данные:
1. Лог событий IDS/IPS(за период 14:00–16:00):

14:15:23 — [ALERT] Suspicious outbound connection to 185.123.45.67:443 (port scan pattern)
14:47:12 — [ALERT] SQL injection attempt on webserver (URL: /search?q=' OR 1=1--)
15:03:44 — [ALERT] Multiple failed SSH logins from 192.168.5.100 (5 attempts in 30 sec)
15:30:18 — [ALERT] Unusual DNS query volume (100+ requests/sec to random subdomains)

2. Отчёт системного администратора:

- На веб-сервере обнаружено изменение файла index.html (добавлена скрытая ссылка).
- В логах БД зафиксированы запросы на чтение таблицы users (10 000 строк).
- Несколько рабочих станций показывают высокую загрузку ЦП и сетевую активность.

3. Информация от пользователей:

- 3 сотрудника сообщили о «странных всплывающих окнах» в браузере.
- 1 пользователь заметил вход в почту с неизвестного устройства.

Задание:

1. **Выявите не менее 4 типов атак**, зафиксированных в логах и отчётах. Для каждой:
- укажите **название атаки** (термин);
- опишите **механизм реализации** (1–2 предложения);
- назовите **уязвимость/слабость**, которую использовал злоумышленник.
2. **Определите цепочку событий** (хронологию атак). Предположите, как злоумышленник мог продвигаться по сети (от начальной точки до финального действия).
3. **Предложите 3–4 срочные меры** для:
- остановки текущей атаки;
- локализации заражённых узлов;
- предотвращения повторного вторжения.
4. **Разработайте 2–3 долгосрочные меры** по усилению защиты:
- для веб-сервера;
- для почтовой системы;
- для рабочих станций.

Пример правильного ответа.

1. Выявленные атаки:

- **Сканирование портов** (14:15:23):
- Механизм: злоумышленник отправляет пакеты на разные порты, чтобы найти открытые сервисы.
- Уязвимость: отсутствие файрвола, разрешающий правила для внешних подключений.
- **SQL-инъекция** (14:47:12):
- Механизм: внедрение вредоносного SQL-кода в параметр q для обхода аутентификации.

- Уязвимость: отсутствие фильтрации ввода, слабые настройки веб-приложения.
- **Брутфорс SSH** (15:03:44):
- Механизм: перебор паролей для получения доступа к серверу.
- Уязвимость: слабые пароли, отсутствие блокировки после неудачных попыток.
- **DNS-туннелирование/флуд** (15:30:18):
- Механизм: использование DNS-запросов для передачи данных или перегрузки сервера.
- Уязвимость: отсутствие мониторинга аномального DNS-трафика.

2. Хронология:

1. Сканирование портов → выявление открытых сервисов.
2. SQL-инъекция → компрометация веб-сервера.
3. Брутфорс SSH → попытка захвата сервера.
4. DNS-флуд → отвлечение внимания или передача данных.

3. Срочные меры:

- заблокировать IP 185.123.45.67 на файрволе;
- изолировать веб-сервер и рабочие станции с аномальной активностью;
- сменить пароли всех учётных записей;
- включить двухфакторную аутентификацию (2FA) для SSH и почты.

4. Долгосрочные меры:

- для веб-сервера: внедрить WAF (Web Application Firewall), регулярно обновлять ПО;
- для почты: включить 2FA, фильтровать подозрительные вложения;
- для рабочих станций: установить EDR-решение, проводить обучение пользователей.

Критерии оценки (максимум 28 баллов).

- **Часть 1** (выявление атак) — до 12 баллов (3 балла за каждую атаку: 1 — название, 1 — механизм, 1 — уязвимость).
- **Часть 2** (хронология) — до 4 баллов (логичность, соответствие данным).
- **Часть 3** (срочные меры) — до 6 баллов (практичность, полнота).
- **Часть 4** (долгосрочные меры) — до 6 баллов (конкретика, охват систем).

Задание 9.

В упрощённой «азбуке Морзе» для цифр используются последовательности из точек (·) и тире (–) длиной ровно 4 символа. Например:

5.0 = · · · ·

6.1 = · – – –

Необходимо ответить на вопросы:

1. Сколько разных цифр можно закодировать такими последовательностями?
2. Можно ли добавить ещё одну цифру, не увеличивая длину кода?
3. Если для каждой цифры использовать ровно 5 символов, сколько цифр удастся закодировать?

Ответы

1.2^4=16 комбинаций → можно закодировать 16 цифр.
2.Да, так как 16>10.
3.2^5=32 комбинации → 32 цифры.

Критерии оценки

Вопросы 1–3: по 1 баллу.
Максимум: 3 балла.

Задание 10.

Вы — специалист по информационной безопасности компании *SecureNet*. Вам необходимо проанализировать текущую конфигурацию сетевого взаимодействия и предложить меры по усилению защиты данных.

Исходная ситуация:

В компании используются следующие сервисы и протоколы:

-веб-сайт (HTTP/HTTPS);
-почтовый сервер (SMTP, IMAP);
-удалённое администрирование (SSH);
-VPN для доступа сотрудников в корпоративную сеть.

При аудите выявлены следующие факты:

1.Веб-сайт частично работает по HTTP (некоторые страницы не перенаправляются на HTTPS).
2.На почтовом сервере используется устаревшая версия TLS 1.0.
3.Для SSH применяются ключи длиной 1 024 бита.
4.VPN-сервер использует протокол PPTP.
5.В сети не настроен механизм проверки сертификатов (OCSP/CRL).

Задание:

1.**Укажите уязвимости** в текущей конфигурации (по каждому из 5 пунктов). Кратко поясните, какие атаки возможны из-за каждой уязвимости (1–2 предложения).

2.**Предложите конкретные меры** по устранению каждой уязвимости.
Укажите:
- какие протоколы/версии следует использовать вместо текущих;
- какие параметры конфигурации нужно изменить (длины ключей, алгоритмы и т. п.);
- дополнительные механизмы защиты (если требуются).
3.**Объясните**, почему важно регулярно обновлять версии протоколов и алгоритмов шифрования. Приведите 2–3 аргумента.

Пример правильного ответа (кратко)
1.**Уязвимости и атаки:**
•HTTP вместо HTTPS — перехват данных (сниффинг), подмена контента (MITM).
•TLS 1.0 — уязвимости типа POODLE, возможность расшифровки трафика.
•SSH-ключи 1 024 бита — подвержены брутфорсу, компрометация учётных записей.
•PPTP — известные уязвимости в MPPE, лёгкий взлом VPN-туннеля.
•Отсутствие OCSP/CRL — использование отозванных сертификатов, MITM-атаки.
2.**Меры устранения:**
•Перевести весь сайт на HTTPS, настроить HSTS.
•Обновить TLS до версии 1.3, отключить устаревшие алгоритмы.
•Сгенерировать SSH-ключи длиной 2 048 бит (RSA) или перейти на Ed25519.
•Заменить PPTP на OpenVPN или IPSec/IKEv2.
•Настроить проверку статуса сертификатов через OCSP или CRL.
3.**Аргументы за обновления:**
•Закрытие известных уязвимостей.
•Повышение стойкости алгоритмов к современным методам взлома.
•Соответствие актуальным стандартам (PCI DSS, GDPR и др.).

Критерии оценки (максимум 21 балл)
Часть 1 (уязвимости + атаки) — до 10 баллов (2 балла за каждый пункт).
Часть 2 (меры устранения) — до 8 баллов (1–2 балла за каждое предложение).
Часть 3 (аргументы за обновления) — до 3 баллов (1 балл за аргумент).

Задание 11.

Вам представлены четыре сценария возможных инцидентов информационной безопасности и фрагменты логов/данных. **Определите:**

1. какой тип атаки реализован в каждом случае;
2. какую уязвимость использовал злоумышленник;
3. какие последствия возможны при успешной реализации атаки.

Известно, что среди ответов есть следующие виды атак: фишинг, SQL-инъекция, DDoS, компрометация учётной записи.

Для каждого сценария:

1.Назовите тип атаки (используйте общепринятые термины: фишинг, DDoS, SQL-инъекция, XSS, брутфорс, спуфинг и т. п.).

2.Укажите, какая уязвимость или слабое место системы позволило атаке состояться.

3.Опишите 1–2 возможных последствия (утечка данных, отказ сервиса, компрометация учётных записей и т. п.).

4.Предложите 1–2 меры защиты, которые могли бы предотвратить или снизить риск такой атаки.

Сценарии:

Сценарий 1. «Подозрительное письмо».

Пользователь получил письмо от «службы поддержки банка» с просьбой подтвердить данные карты по ссылке. Ссылка ведёт на сайт с адресом, похожим на официальный (например, bank-secure.net вместо bank.ru). При переходе на сайт требуется ввести номер карты, срок действия и CVV-код.

Сценарий 2. «Перегрузка сервера»

Администратор заметил резкий рост числа запросов к веб-серверу. Логи показывают тысячи соединений с разных IP-адресов, направленных на один эндпоинт /api/data. Сервер начал отвечать с задержками, затем перестал отвечать совсем.

Сценарий 3. «Странный запрос»

В логах веб-приложения обнаружен запрос:

GET /search?q=admin' OR '1'='1

После этого злоумышленник получил доступ к данным всех пользователей, включая пароли (хранились в незашифрованном виде).

Сценарий 4. «Неизвестный вход»

Пользователь обнаружил в истории входов в свой почтовый аккаунт запись:

- Устройство: iPhone 14;
- Местоположение: Токио, Япония;

- Время: 03:17 UTC (пользователь в это время спал в Москве).
  Пароль от почты не менялся, двухфакторная аутентификация не включена.

Пример правильного ответа.
Сценарий 1:

1. Тип атаки: **фишинг** (поддельный сайт для кражи платёжных данных).
2. Уязвимость: доверчивость пользователя + отсутствие проверки URL (визуальное сходство доменов).
3. Последствия: кража данных карты, финансовые потери.
4. Меры защиты:

- обучение пользователей (проверять URL, не переходить по подозрительным ссылкам);
- использование антифишинговых фильтров в почте.

Сценарий 2:

1. Тип атаки: **DdoS** (распределённая атака на отказ сервиса).
2. Уязвимость: отсутствие защиты от флуда (нет лимитов на запросы, нет CDN/файрвола).
3. Последствия: недоступность сервиса, потери для бизнеса.
4. Меры защиты:

- настройка лимитов на число запросов с одного IP;
- использование CDN с защитой от DDoS (например, Cloudflare).

Сценарий 3:

1. Тип атаки: **SQL-инъекция** (внедрение вредоносного кода в запрос).
2. Уязвимость: отсутствие фильтрации ввода в параметре q, хранение паролей в открытом виде.
3. Последствия: утечка данных пользователей, компрометация учётных записей.
4. Меры защиты:

- валидация и санитизация входных данных;
- хранение паролей с хешированием (bcrypt, Argon2).

Сценарий 4:

1. Тип атаки: **компрометация учётной записи** (взлом через украденный/подобранный пароль).
2. Уязвимость: отсутствие двухфакторной аутентификации (2FA), слабый пароль.
3. Последствия: доступ к личной переписке, кража конфиденциальных данных.
4. Меры защиты:

- включение 2FA (SMS/приложение-аутентификатор);
- регулярная смена паролей, использование менеджеров паролей.

Критерии оценивания (максимум 20 баллов)

- **Сценарий 1** — до 5 баллов (тип атаки + уязвимость + последствия + меры защиты).
- **Сценарий 2** — до 5 баллов.
- **Сценарий 3** — до 5 баллов.
- **Сценарий 4** — до 5 баллов.

По 1–1,5 балла за каждый элемент ответа в зависимости от полноты и точности.

Задание 12.

Напишите команду iptables, которая **запрещает** все входящие пакеты с IP-адреса 192.168.1.100.

Ответ:

bash

```
iptables -A INPUT -s 192.168.1.100 -j DROP
```

Пояснение:

-s 192.168.1.100 — источник пакета;

-j DROP — отбросить пакет без ответа.

Критерии оценивания: за правильный ответ — 6 баллов.

Задание 13.

В 2021 году произошла крупная утечка паролей, известная как RockYou2021. В ней фигурировало около 8,4 млрд уникальных паролей, что стало на тот момент крупнейшей утечкой в истории. Файл с паролями объёмом около 100 ГБ был опубликован на хакерском форуме пользователем с ником RockYou2021. Эта утечка стала одним из крупнейших инцидентов того времени и подчеркнула важность защиты данных.

Вам предоставлен фрагмент лог-файла веб-сервера компании *SecureTech* за 12.03.2025:

192.168.1.100 - - [12/Mar/2025:14:23:15 +0300] "GET /login.php?user=admin' OR '1'='1 HTTP/1.1" 200 1245
192.168.1.100 - - [12/Mar/2025:14:23:18 +0300] "POST /login.php HTTP/1.1" 403 342

192.168.1.101 - - [12/Mar/2025:14:24:01 +0300] "GET /index.php?file=../../../../etc/passwd HTTP/1.1" 404 289
192.168.1.102 - - [12/Mar/2025:14:25:33 +0300] "GET / HTTP/1.1" 200 1567
192.168.1.100 - - [12/Mar/2025:14:26:02 +0300] "GET /api/data?id=<script>alert('XSS')</script> HTTP/1.1" 200 984

Задание:

1.Определите **тип каждой атаки**, зафиксированной в логах (всего 4 различные атаки). Кратко опишите механизм каждой из них (1–2 предложения).
2.Укажите, **какие уязвимости** веб-приложения позволили провести эти атаки.
3.Предложите **по 1–2 меры защиты** для каждой уязвимости (на уровне кода, конфигурации сервера или политик безопасности).
4.Объясните, почему код <script>alert('XSS')</script> в запросе может представлять угрозу, даже если страница отображается корректно.

Пример правильного ответа.
1.**Типы атак:**
•SQL-инъекция (user=admin' OR '1'='1) — внедрение SQL-кода для обхода аутентификации.
•Попытка LFI (../../../../etc/passwd) — доступ к файлам ОС через уязвимость включения файлов.
•XSS (<script>alert(...)</script>) — внедрение JS-кода в ответ сервера.
•Возможная попытка брутфорса (множественные запросы к /login.php).
2.**Уязвимости:**
•Отсутствие фильтрации ввода в SQL-запросах.
•Небезопасная обработка параметров включения файлов (LFI).
•Отсутствие санации вывода (XSS).
•Слабая защита от переборных атак на авторизацию.
3.**Меры защиты:**
•Для SQL-инъекций: использование подготовленных запросов (Prepared Statements).
•Для LFI: запрет абсолютных путей, белый список разрешённых файлов.
•Для XSS: фильтрация/экранирование спецсимволов, заголовок Content-Security-Policy.
•Для брутфорса: ограничение числа попыток, CAPTCHA.
4.**Угроза XSS:** код может выполняться у других пользователей, красть «куки», перенаправлять на фишинговые страницы.

Критерии оценивания (максимум 20 баллов).

1. **Часть 1** (4 типа атак + механизм) — до 8 баллов (2 балла за каждый тип).
2. **Часть 2** (уязвимости) — до 4 баллов (1 балл за каждую).
3. **Часть 3** (меры защиты) — до 6 баллов (1–2 балла за набор мер по каждой уязвимости).
4. **Часть 4** (объяснение XSS) — до 2 баллов.

Задание 14.

Робот по имени Эйдж «читает» QR-коды размером 3×3 клетки. Каждая клетка — либо чёрная (1), либо белая (0).

Ответьте на вопросы:

1. Сколько всего разных QR-кодов такого размера?
2. Сколько кодов, где ровно 4 чёрные клетки?
3. Робот понимает код, только если в нём есть хотя бы один «квадрат» 2×2 из чёрных клеток. Сколько таких кодов?
4. Придумайте правило кодирования, чтобы по коду 3×3 можно было однозначно определить цифру от 0 до 8 (всего 9 вариантов). Опишите правило и приведите примеры для 0, 1, 8.

Ответ:

1. $2^9=512$.
2. $C(9,4)=126$.
3. Квадратов 2×2 в матрице 3×3 — 4 (углы). Для каждого считаем коды, где он полностью чёрный, а остальные клетки — любые. Потом вычитаем пересечения (когда два квадрата 2×2 перекрываются). Итого:
$4 \square 25 - 4 \square 22 + 1 = 113$ (подробный перебор).

<u>Критерии оценивания:</u>

Вопрос 1: 1 балл.
Вопрос 2: 2 балла.
Вопрос 3: 3 балла (нужно обосновать выбор позиций для повторяющейся цифры).
Вопрос 4: 2 балла (подсчёт сочетаний без повторений).

Максимум за задание — 8 баллов.

Задание 15.

Для открытия сейфа нужно ввести четырехзначный код. Цифры могут повторяться. **Ответьте на следующие вопросы:**

1. Сколько всего существует возможных комбинаций кода для данных условий?
2. Сколько может быть возможных комбинаций, где все цифры разные?
3. Сколько комбинаций, где ровно две цифры одинаковые (остальные — разные)?
4.Сколько комбинаций, где цифры идут строго по возрастанию (например, 1234, 0125)?

Ответы:

1. 104=10000.
2. 10□9□8□7=5040.
3.Выбираем цифру-повтор (10 вариантов), позиции для неё ($C(4,2)=6$), оставшиеся две цифры (9□8): 10□6□9□8=4320.
4. Выбираем 4 разные цифры из 10 и упорядочиваем их единственным образом: $C(10,4)=210$.

<u>Критерии оценивания:</u>

Вопрос 1: 1 балл.
Вопрос 2: 2 балла.
Вопрос 3: 3 балла (нужно обосновать выбор позиций для повторяющейся цифры).
Вопрос 4: 2 балла (подсчёт сочетаний без повторений).
Максимум за задание — 8 баллов.

Задание 16.

В адрес олимпиады по информационной безопасности пришло зашифрованное сообщение: Ф В М Е Ж Т И В Ф Ю

Найдите исходное сообщение, если известно, что шифрообразование заключалось в следующем. Пусть X_1, X_2 — корни трехчлена X^2+3X+1. К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавлялось значение многочлена $f(X)=X^6+3X^5+X^4+X^3+4X^2+3$, вычисленное либо при $X=X_1$, либо при $X=X_2$ (в неизвестном нам порядке), а затем полученное число заменялось соответствующей ему буквой.

Формат вывода: текстовое сообщение.

Ответ: ТАКДЕРЖАТЬ

Пояснение: легко увидеть, что $f(x)=(X^2+3X+1)(X^4+X+1)+2$. Отсюда следует, что $f(X)=f(X^2)=2$, где X_1, X_2 — корни многочлена X2+3X+1. Получаем:

Буква ш.с.	**Ф**	**В**	**М**	**Е**	**Ж**	**Т**	**И**	**В**	**Ф**	**Ю**
Номер	**22**	**3**	**14**	**7**	**8**	**20**	**10**	**3**	**22**	**32**

Номер	**20**	**1**	**12**	**5**	**6**	**18**	**8**	**1**	**20**	**30**
Буква ш.с.	**Т**	**А**	**К**	**Д**	**Е**	**Р**	**Ж**	**А**	**Т**	**Ь**

Критерии оценивания: максимум 10 баллов.

Задание 17.

Установите, можно ли создать проводную телефонную сеть связи, состоящую из 993 абонентов, каждый из которых был бы связан ровно с 99 другими.

Формат вывода: ДА/НЕТ.

Ответ: НЕТ

Критерии оценивания: 5 баллов.

Задание 18.

Чтобы запомнить периодически меняющийся пароль в ЭВМ, математики придумали следующий способ. При известном числе a (например, номере месяца в году), пароль представляет собой первые шесть цифр наименьшего решения уравнения:

$$a(x^2-1)=\sqrt{1+\frac{x}{a}},\ \text{при } 0<a<1$$

Число меньшей значности дополняется справа необходимым числом нулей. Решите такое уравнение при произвольном a>0.

Ответ: при $0 < a < 1$ $x = \dfrac{1+\sqrt{4a^2+1}}{2a}$

$$x_1 = \frac{1+\sqrt{4a^2+1}}{2a}, x_2 = \frac{-\sqrt{4a^2-3}-1}{2a}$$ при $a \geq 1$

Критерии оценивания: максимум 10 баллов.

Задание 19.

Буквы русского алфавите занумерованы в соответствии с таблицей.

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

Для зашифрования сообщения, состоящего их n букв, выбирается ключ К — некоторая последовательность из n букв приведенного выше алфавита. Зашифрование каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма.

Прочтите шифрованное сообщение: **Р Б Ь Н Т С И Т С Р Р Е З О Х**, если известно, что шифрующая последовательность не содержала никаких букв, кроме А,Б и В.

Формат вывода: осмысленное сообщение.

Ответ: НАШКОРРЕСПОНДЕНТ/ НАШ МОРОЗ ПОПОВ ЕМУ/НАШ МОРОЗ ПОМОГ ЕМУ.

Пояснение: каждую букву шифрованного сообщения расшифруем в трех вариантах, предполагая последовательно, что соответствующая буква шифрующей последовательности есть буква А, Б или В:

Шифрованное сообщение	**Р**	**Б**	**Ь**	**Н**	**П**	**Т**	**С**	**И**	**Т**	**С**	**Р**	**Р**	**Е**	**З**	**О**	**Х**
Вариант А	**П**	**А**	**Щ**	**М**	**О**	**С**	**Р**	**З**	**С**	**Р**	**П**	**П**	**Д**	**Ж**	**Н**	**Ф**
Вариант Б	**О**	**Я**	**Ш**	**Л**	**Н**	**Р**	**П**	**Ж**	**Р**	**П**	**О**	**О**	**Г**	**Е**	**М**	**У**
Вариант В	**Н**	**Ю**	**Ч**	**К**	**М**	**П**	**О**	**Е**	**П**	**О**	**Н**	**Н**	**В**	**Д**	**Л**	**Т**

Выбирая из каждой колонки полученной таблицы ровно по одной букве, находим осмысленное сообщение: **НАШКОРРЕСПОНДЕНТ**, которое и является искомым.

Замечание: из полученной таблицы можно было найти такое сообщение как: **НАШ МОРОЗ ПОПОВ ЕМУ**, которое тоже может быть осмысленным.

А если предположить одно искажение в шифрованном соощении (например, в качестве 11-ой буквы была бы принята не буква **Р**, а буква **П**), то, наряду с правильным вариантом, можно получить следующий:

НАШ МОРОЗ ПОМОГ ЕМУ

Число всех различных вариантов исходных сообщенийбез ограничений на осмысленность равно 3^{16} или 43046721, т. е. более 40 миллионов.

Критерии оценивания: максимум 15 баллов.

Задание 20.

Вам предоставлен **фрагмент дизассемблированного кода** (условный псевдоассемблер) и **краткое описание поведения** программы. Ваша задача — понять алгоритм работы и ответить на вопросы.

Фрагмент кода (с комментариями):

```
start:
    mov eax, [input_length]    ; загружаем длину введённой строки
    cmp eax, 8                 ; сравниваем с числом 8
    jne reject                 ; если не равно — переход к reject


    mov esi, input_string      ; указатель на введённую строку
    mov edi, secret_key        ; указатель на «секретный ключ»
    mov ecx, 8                 ; длина для сравнения — 8 байт
    rep cmpsb                  ; сравниваем 8 байт строки с secret_key
    jne reject                 ; если не совпадают — переход к reject


accept:
    call print_success         ; выводим сообщение об успехе
    jmp exit

reject:
    call print_failure         ; выводим «Access denied!»
```

```
    jmp exit


exit:
    ret
```

Описание поведения программы:
- Программа принимает на вход текстовую строку.
- Если строка **ровно 8 символов** и **совпадает с неким «секретным ключом»**, выводится сообщение об успехе.
- В противном случае выводится «Access denied!».

Задание

Ответьте на вопросы (кратко, по 1–3 предложения на каждый):

1. **Какова длина «правильного» входного значения?** Обоснуйте ответ, опираясь на код.
2. **Как программа проверяет совпадение введённой строки с «секретным ключом»?** Опишите последовательность действий (используйте названия команд из фрагмента).
3. **Что произойдёт, если ввести строку длиной 7 символов?** Какой участок кода будет выполнен и почему?
4. **Предположите, в каком виде может храниться** secret_key **в бинарном файле.** Где (в каких секциях PE/ELF) его можно попытаться найти?
5. **Назовите 2 инструмента**, которые помогут извлечь secret_key из исполняемого файла без запуска программы. Кратко поясните, как они работают в этом контексте.

Пример правильного ответа

1. Длина правильного входного значения — 8 символов. В коде есть сравнение cmp eax, 8 и условие перехода jne reject, если длина не равна 8.
2. Программа:
- загружает указатель на введённую строку (mov esi, input_string);
- загружает указатель на secret_key (mov edi, secret_key);
- устанавливает счётчик на 8 байт (mov ecx, 8);
- выполняет побайтовое сравнение (rep cmpsb);
- если есть несовпадение, переходит к reject.

3. Если ввести 7 символов, программа перейдёт к reject, так как cmp eax, 8 даст «не равно», и сработает jne reject.

4.secret_key может храниться в секции .data или .rodata (как константа). В PE-файле это обычно секция с атрибутом «читаемый, неисполняемый».
5.Инструменты:
•strings — ищет читаемые строки в бинарнике, может вывести secret_key, если он представлен в текстовом виде;
•Ghidra — дизассемблер, позволяет просмотреть содержимое секций .data/.rodata и найти значение secret_key.

Критерии оценивания (максимум 20 баллов).
Вопрос 1 — 3 балла (ответ + обоснование).
Вопрос 2 — 5 балла (чёткое описание последовательности команд).
Вопрос 3 — 4 балла (точный сценарий + ссылка на код).
Вопрос 4 — 4 балла (предположение + обоснование места хранения).
Вопрос 5 — 4 балла (2 инструмента + краткое пояснение).