ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ

Разбор заданий муниципального этапа всероссийской олимпиады школьников по информатике профиль «Информационная безопасность» для 9 классов

2025/2026 учебного года в Свердловской области

Разработчик –
Стариченко Евгений Борисович,
АНПОО «Колледж Цифровых Технологий»

Задание 1. (1 балл)

Представьте, что вы работаете в школе и отвечаете за обработку персональных данных учащихся. Вам необходимо подготовить документ о согласии на обработку персональных данных для родителей учеников. Выберите обязательные пункты, которые должны быть включены в такой документ согласно законодательству.

а. Цель обработки персональных данных
б. Перечень обрабатываемых данных
в. Срок действия согласия
г. Порядок отзыва согласия
д. Подписи сторон

Обязательные пункты документа о согласии на обработку персональных данных:

а. Цель обработки персональных данных
б. Перечень обрабатываемых данных
в. Срок действия согласия
г. Порядок отзыва согласия
д. Подписи сторон

Задание 2. (2 балла)

Перечислите не указанные в задании 1 обязательные пункты документа о согласии на обработку персональных данных.

Обязательно должны быть указаны:

- наименование или ФИО и адрес оператора;
- перечень действий с данными;
- способы обработки данных.

Задание 3. (2 балла)

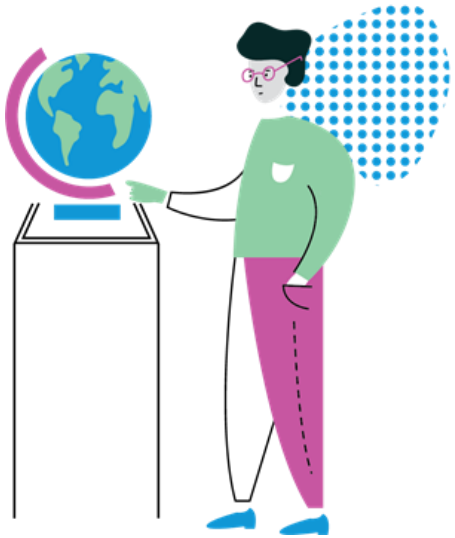
Ученик 9 класса разместил в социальной сети фотографию своего одноклассника с указанием адреса проживания, номера школы и класса. Через некоторое время он получил сообщение от незнакомого человека с просьбой о встрече.

а. Какие нарушения законодательства о персональных данных были допущены?

б. Какие последствия могут возникнуть в результате таких действий?

в. Какие меры предосторожности следует соблюдать при размещении информации в социальных сетях?

г. Куда можно обратиться за защитой своих прав в случае нарушения конфиденциальности персональных данных?



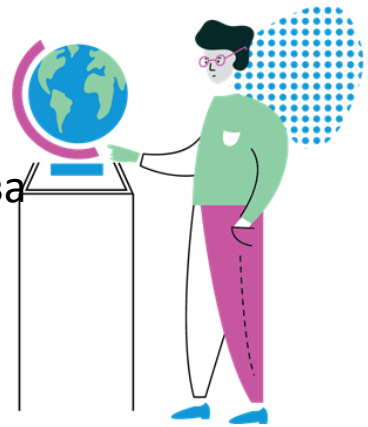
Задание 3. (2 балла)
Анализ ситуации

а. Нарушения:
- публикация информации, позволяющей идентифицировать личность

б. Возможные последствия:
- кража личных данных
- мошенничество
- преследование
- опасность для личной безопасности

в. Меры предосторожности:
- не указывать личную информацию
- использовать настройки приватности
- не добавлять незнакомцев в друзья
- сообщать родителям о подозрительных сообщениях

г. Куда обращаться:
- к родителям или законным представителям
- в администрацию социальной сети
- в правоохранительные органы
- в Роскомнадзор при нарушении законодательства



Задание 4. (1 балл)

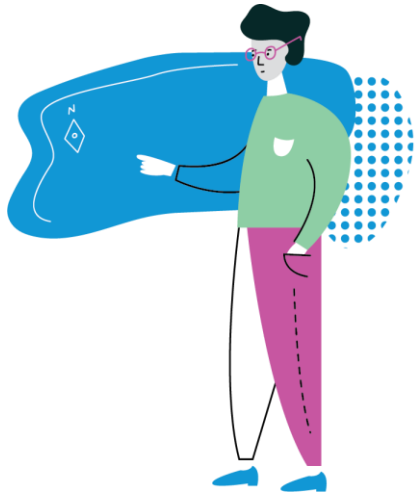
Вы нашли в интернете предложение о быстром заработке с минимальными вложениями.

а. Какие риски связаны с подобными предложениями?
б. Как проверить надёжность такого предложения?
в. Какие действия помогут избежать мошенничества?

а. Риски:
- Потеря денег
- Кража личных данных
- Мошенничество

б. Проверка надёжности:
- Поиск отзывов
- Проверка официального сайта
- Консультация с родителями

в. Меры предосторожности:
- Не вкладывать деньги
- Не сообщать личные данные
- Обсудить предложение с родителями



Задание 5. (4 балла)

Вам необходимо настроить политику безопасности для нового пользователя, которому вы даёте доступ к своему серверу под управлением ОС на основе ядра Linux. Перечислите основные шаги по настройке безопасного аккаунта.

Основные шаги по настройке безопасного аккаунта
- создание пользователя;
- назначение группы;
- установка пароля;
- настройка прав доступа;
- ограничение доступа к системным файлам.

Задание 6. (4 балла)

В организации возникла необходимость ограничить доступ пользователей к определённым системным командам.

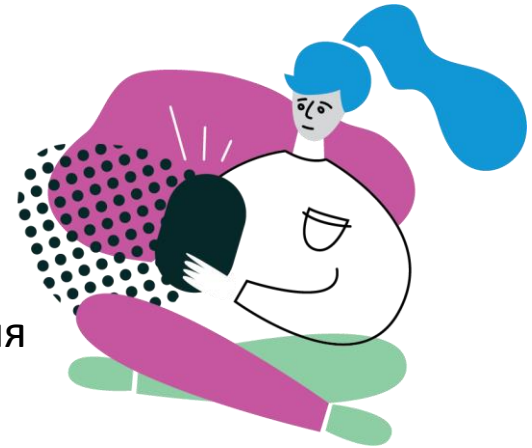
а. Какие инструменты Linux можно использовать для ограничения доступа?
б. Как настроить список разрешённых команд для пользователя?
в. Какие риски могут возникнуть при неправильной настройке?
г. Как проверить корректность настроек безопасности?

а. Инструменты для ограничения доступа:
- /etc/sudoers
- SELinux/AppArmor
- группы пользователей

б. Настройка списка команд:
- редактирование файла sudoers
- создание алиасов команд
- ограничение доступа через shell

в. Возможные риски:
- потеря доступа к системе
- нарушение работоспособности приложений
- уязвимости безопасности

г. Проверка настроек:
- тестирование доступа от имени пользователя
- проверка логов аудита
- использование команд id, groups, sudo -l



Задание 7. (3 балла)

Рассмотрите схему сети:

Опишите процесс передачи файла размером 1 МБ от компьютера 1 к компьютеру 2.

- файл разбивается на пакеты (обычно 1500 байт);
- каждый пакет получает IP-заголовок с адресами отправителя и получателя;
- маршрутизаторы определяют оптимальный путь для каждого пакета;
- протокол TCP обеспечивает надежность передачи;
- на компьютере Б пакеты собираются в исходном порядке.

Задание 8. (3 балла)

В организации возникла проблема с медленной передачей файлов между отделами. Есть предположение, что проблема в маршрутизации.

а. Какие факторы могут влиять на скорость маршрутизации?

б. Какие протоколы маршрутизации можно использовать для оптимизации?

в. Как проверить правильность настройки маршрутизации?

г. Какие инструменты можно использовать для мониторинга маршрутизации?

а. Факторы влияния:

- загруженность каналов связи;
- правильность построения маршрутов;
- нагрузка на маршрутизаторы;
- конфигурация сетевых устройств.

б. Протоколы для оптимизации:

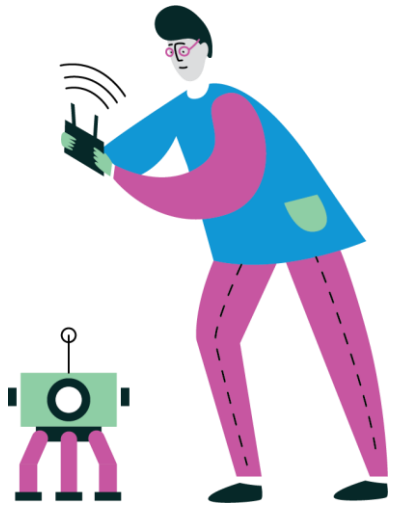
- RIP (Routing Information Protocol);
- OSPF (Open Shortest Path First);
- BGP (Border Gateway Protocol).

в. Проверка настройки:

- команда ping;
- команда traceroute;
- проверка таблиц маршрутизации.

г. Инструменты мониторинга:

- утилита netstat;
- программа Wireshark;
- системные журналы (логи).



Задание 9. (2 балла)

Вы получили от знакомого друга записку следующего содержания:

5111521453421411246532115111334261534342334443632311244262614
6

Расшифруйте послание, используя матрицу:
Пробелы в шифре и в исходной фразе удалены.

	1	2	3	4	5	6
1	а	б	в	г	д	е
2	ё	ж	з	и	й	к
3	л	м	н	о	п	р
4	с	т	у	ф	х	ц
5	ч	ш	щ	ъ	ы	ь
6	э	ю	я	.	,	?

Зашифрованная фраза «дай списать задание по информатике.»

Задание 10. (4 балла)

Предложите три варианта усовершенствования (усложнения) шифра из задания 9.

- изменить порядок символов алфавита;
- изменить нумерацию ячеек (использовать трёхзначные/шестнадцатеричные числа)
- использовать матрицу переменного размера (размер матрицы становится частью ключа, периодически менять матрицу в процессе шифрования). Вариант — использование нескольких матриц с разным порядком следования символов и периодической сменой их в процессе шифрования;
- двойное шифрование (например, сначала изменить порядок букв с помощью шифра со сдвигом, потом зашифровать по матрице);
- динамическое перемещение символов (например, базовая матрица заполняется по алфавиту, выбирается ключ-число, через определенное количество символов происходит сдвиг символов, правила сдвига определяются ключом).

Задание 11. (5 баллов)

Другой ваш знакомый друг, с которым у вас договорённость использовать для шифрования ключевое слово, соответствующее названию дня недели отправки письма, прислал 26.09.2025 года следующее сообщение:

ЭЯЙЦЦЦТЛБДТЛЪАБСБЦЫЗТЮВБЕЫЕСФДЕЯЧГНФМЫМ

Определите тип шифра и расшифруйте сообщение. В ответе укажите способ шифрования, ключевое слово и исходное сообщение. Учитывайте, что пробелы в исходном сообщении удалены.

Шифр Виженера, ключевое слово — пятница, ответ

НАЧИНАТЬВСЕГДАСТОИТСТОГОЧТОСЕЕТСОМНЕНИЯ

Начинать всегда стоит с того, что сеет сомнения

Задание 12. (5 баллов)

Проанализируйте представленный фрагмент сетевого трафика и ответьте на вопросы.

12:35:45.123 IP 192.164.1.100:54321 > 77.88.8.8:53
12:35:45.125 IP 192.164.1.100:54322 > 77.88.8.8:53
12:35:45.127 IP 192.164.1.100:54323 > 77.88.8.8:53

а. Какой протокол используется в данном трафике?
б. Определите IP-адрес отправителя и получателя.
в. Что можно сказать о характере трафика?
г. Почему порты отправителя разные, а порт получателя одинаковый?

а. DNS (порт 53)
б. отправитель: 192.164.1.100, получатель: 77.88.8.8 (Яндекс DNS)
в. это DNS-запросы
г. порт 53 — стандартный порт DNS-сервера, а отправитель использует эфемерные порты

Задание 13. (4 балла)

Как называется атака, при проведении которой злоумышленники подменяют настройки DNS и перенаправляют пользователей на вредоносные сайты? В чём она заключается и как проводится?

Название атаки «Перехват DNS-запросов». Атака заключается в замене ответов настоящего DNS-сервера на вредоносные IP-адреса.
Когда вы вводите адрес в поисковую строку, веб-браузер ищет информацию о веб-странице в кэше локальной памяти (если вы ранее уже посещали эту страницу) или отправляет DNS-запрос на сервер системы доменных имен (обычно предоставленный интернет-провайдером). Процесс обмена данными между браузером и сервером системы доменных имен наиболее уязвим для атаки, поскольку данные передаются в незашифрованном виде. Именно в этот момент злоумышленники перехватывают запрос и подменяют ответ. Киберпреступники используют четыре различных способа перехвата DNS-запроса: локально, на уровне роутера, на уровне DNS-сервера и по типу man-in-the-middle («человек посередине»).

Задание 14. (4 балла)

Вы получили по электронной почте письмо от знакомого друга, содержащее следующую запись: `10.12.74.22/29`.

Что она обозначает? Перечислите сведения, которые с её помощью можно получить.

Запись 10.12.74.22/29 — IP адрес.

- его сетевая маска 255.255.255.248 = 29
- адрес сети 10.12.74.16/29
- широковещательный адрес 10.12.74.23
- всего хостов в сети 6
- доступные адреса хостов от 10.12.74.17 до 10.12.74.22

Задание 15. (5 баллов)

Что означает приведённая ниже запись? Дайте подробный ответ.
ufw allow 3000:3100/tcp
ufw deny 3000:3100/udp

Данная запись является командами настройки брандмауэра ufw.
`ufw allow 3000:3100/tcp` — разрешает входящий TCP-трафик через диапазон портов от 3000 до 3100 включительно
`ufw deny 3000:3100/udp` — запрещает входящий UDP-трафик через тот же диапазон портов (3000-3100)
Т.е. эти две команды создают следующую конфигурацию:
– любой TCP-трафик в диапазоне портов 3000-3100 будет пропущен через файрвол;
– любой UDP-трафик в этом же диапазоне портов будет заблокирован.
Такая конфигурация может быть использована для сервисов, которые:
– используют TCP для нормальной работы;
– не должны использовать UDP в этом диапазоне портов (для безопасности);
– хотят предотвратить возможные атаки через UDP-протокол.

ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ ИНФОРМАТИКА ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ

Задание 16. (5 баллов)

Что означает приведённая ниже запись? Дайте подробный ответ.

iptables -A INPUT -s 11.22.121.0/24 -j REJECT
iptables -A OUTPUT -d 31.13.78.35 -j DROP

Данная запись является командами настройки брандмауэра iptables

iptables -A INPUT -s 11.22.121.0/24 -j REJECT — добавляет правило в цепочку INPUT (входящий трафик). В результате все входящие пакеты из подсети 11.22.121.0/24 будут отклонены, и отправитель получит уведомление о том, что его пакеты не приняты.

iptables -A OUTPUT -d 31.13.78.35 -j DROP — добавляет правило в цепочку OUTPUT (исходящий трафик). В результате все исходящие пакеты, направленные на IP-адрес 31.13.78.35, будут удалены системой без уведомления отправителя.

Задание 17. (4 балла)

Рассмотрите фрагмет трафика:

13:22:15.456 TCP 192.168.1.50:80 -> 192.168.1.10:443

13:22:16.457 TCP 192.168.1.50:80 -> 192.168.1.10:443

13:22:17.458 TCP 192.168.1.50:80 -> 192.168.1.10:443

а. Почему данный фрагмент может быть подозрительным?

б. Какие действия следует предпринять?

а. попытка передачи HTTP-трафика (порт 80) на HTTPS-порт (443) может указывать на атаку;

б. проверить источник трафика, заблокировать подозрительный IP.

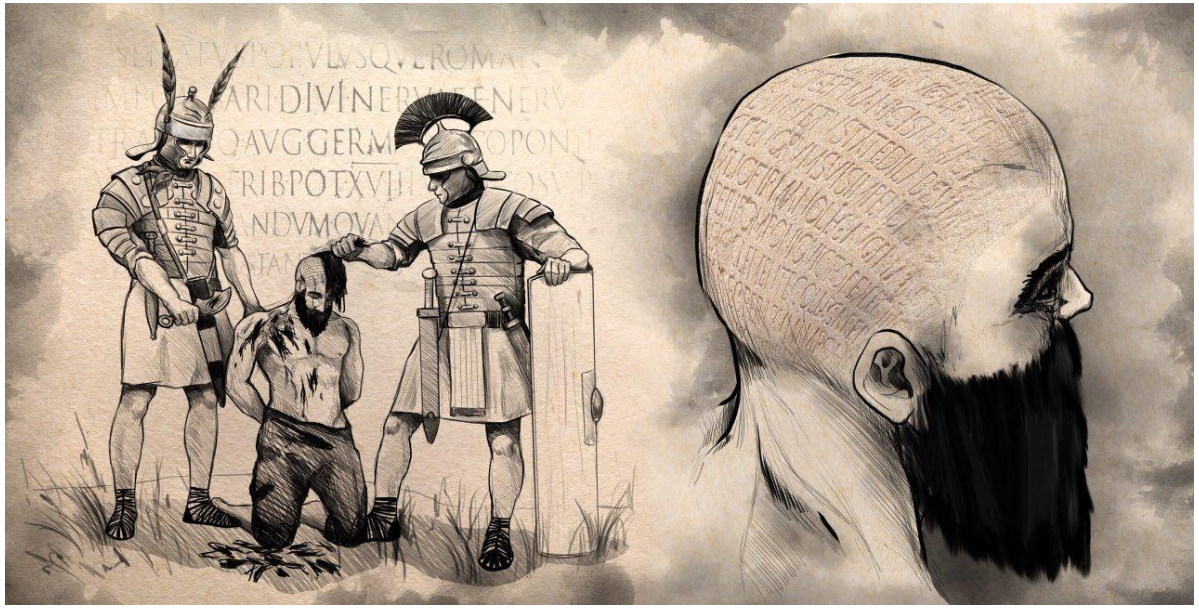
Задание 18. (6 баллов)

Напишите команду, с помощью которой можно заблокировать SSH-соединения с хоста 10.10.10.10.

iptables -A INPUT -p tcp --dport ssh -s 10.10.10.10 -j DROP
или
ufw deny from 10.10.10.10 to any port 22

Задание 19. (2 балла)

Какое отношение происходящее на картинке имеет к защите информации?

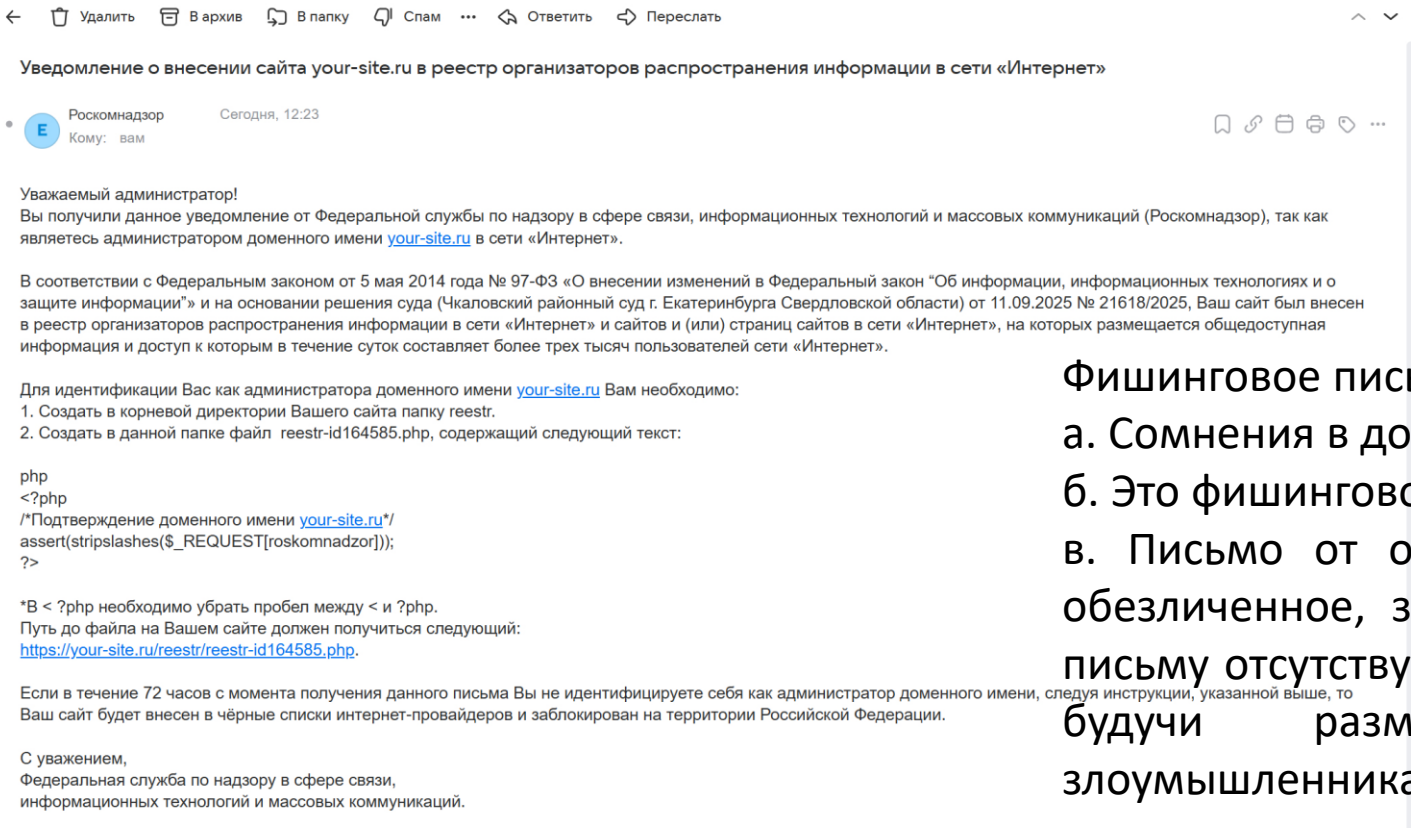


В Римской империи для доставки сообщения выбирали раба, голову которого брили, а затем с помощью татуировки наносили текст. После того, как волосы отрастали, раба отправляли адресату. Получатель сообщения снова обривал голову раба и читал сообщение.

Этот метод сокрытия информации называется «стеганография» (от греч. στεγανός — скрытый + γράφω — пишу; буквально «тайнопись») — технология, позволяющая спрятать передаваемые данные в некотором контейнере, скрыв сам факт передачи информации.

Задание 20. (4 балла)

Вы получили письмо следующего содержания:



Удалить В архив В папку Спам Ответить Переслать

Уведомление о внесении сайта your-site.ru в реестр организаторов распространения информации в сети «Интернет»

Роскомнадзор Сегодня, 12:23
Кому: вам

Уважаемый администратор!
Вы получили данное уведомление от Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), так как являетесь администратором доменного имени your-site.ru в сети «Интернет».

В соответствии с Федеральным законом от 5 мая 2014 года № 97-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”» и на основании решения суда (Чкаловский районный суд г. Екатеринбурга Свердловской области) от 11.09.2025 № 21618/2025, Ваш сайт был внесен в реестр организаторов распространения информации в сети «Интернет» и сайтов и (или) страниц сайтов в сети «Интернет», на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети «Интернет».

Для идентификации Вас как администратора доменного имени your-site.ru Вам необходимо:
1. Создать в корневой директории Вашего сайта папку reestr.
2. Создать в данной папке файл reestr-id164585.php, содержащий следующий текст:

```
php
<?php
/*Подтверждение доменного имени your-site.ru*/
assert(stripslashes($_REQUEST[roskomnadzor]));
?>
```

*В < ?php необходимо убрать пробел между < и ?php.
Путь до файла на Вашем сайте должен получиться следующий:
https://your-site.ru/reestr/reestr-id164585.php.

Если в течение 72 часов с момента получения данного письма Вы не идентифицируете себя как администратор доменного имени, следуя инструкции, указанной выше, то Ваш сайт будет внесен в чёрные списки интернет-провайдеров и заблокирован на территории Российской Федерации.

С уважением,
Федеральная служба по надзору в сфере связи,
информационных технологий и массовых коммуникаций.

а. Какие сомнения оно вызывает?
б. Чем на самом деле является?
в. Приведите свои доводы.

Фишинговое письмо.
а. Сомнения в достоверности.
б. Это фишинговое письмо.
в. Письмо от органа власти, но приветствие в письме обезличенное, заголовок вызывает тревогу, в подписи к письму отсутствуют контактные данные. Приведённый код, будучи размещённым на сайте, позволит злоумышленникам получить к нему доступ.

Это всё!