Тема: 4.3 Основы противодействия киберпреступности.

Учебные вопросы:

1. Сетевой IP-адрес, символьный (DNS) и MAC-адрес сетевого адаптера или порта маршрутизатора.
2. Способы установления IP-адреса и сведений о нем. Возможности установления личности по IP и MAC–адресам.
3. Использование виртуальных частных сетей (VPN) и прокси-серверов (анонимайзеров) в ходе веб-серфинга.
4. Составление запросов операторам электросвязи на получение информации.

1. Сетевой IP-адрес, символьный (DNS) и MAC-адрес сетевого адаптера или порта маршрутизатора

Краткие теоретические сведения:

1.1. Сетевой IP-адрес

Сетевой IP-адрес (Internet Protocol Address) – это уникальный числовой идентификатор конкретного устройства в составе компьютерной сети, построенной на основе протокола TCP/IP. Для работы в сети требуется его глобальная уникальность (для частной сети достаточно, чтобы были исключены совпадения в локальном пространстве). При этом такой идентификатор не обязательно должен быть постоянным (*статическим*). Если используется *динамический* IP, то при перезагрузке компьютера и новом подключении к сети устройство будет получать новый идентификатор.

Каждое устройство, получающее доступ к интернету, всегда имеет IP-адрес. Сведения об этом адресе записываются в логи серверов, которые посещаются пользователями с данного компьютера.

IP-адрес выглядит как комбинация из четырех чисел, разделенных точкой. Этот уникальный идентификатор имеет длину четыре байта. Два первых байта выделены на адрес сети, к которой принадлежит устройство. Третий байт характеризует подсеть, а четвертый является адресом определенного персонального компьютера в указанной подсети. В записи IP-адреса могут присутствовать числа от 0 до 255, которые разделяются точками.

Типы IP-адресов:

А) В зависимости от способа использования

Внешний. Он же «белый», публичный или глобальный. Используется во время доступа в Интернет. Такой IP-адрес является уникальным и именно под ним устройство видят в сети. Так как количество таких идентификаторов ограничено, задействуют технологию NAT. Она позволяет транслировать сетевые IP-адреса из частных в публичные. Для этого применяются маршрутизаторы определенного типа.

По внешним IP-адресам многие интернет-сервисы отслеживают новых и вернувшихся пользователей.

Внутренний. Он же «серый», локальный или частный IP-адрес источника. Не используется во время доступа в Интернет. Работает только в пределах локальной сети (домашней или предоставленной провайдером), и доступ к нему можно получить только другим ее участникам. Для этой цели по умолчанию зарезервированы следующие диапазоны частных IP-адресов:

- 10.0.0.0 – 10.255.255.255;
- 172.16.0.0 – 172.31.255.255;
- 192.168.0.0 – 192.168.255.255.

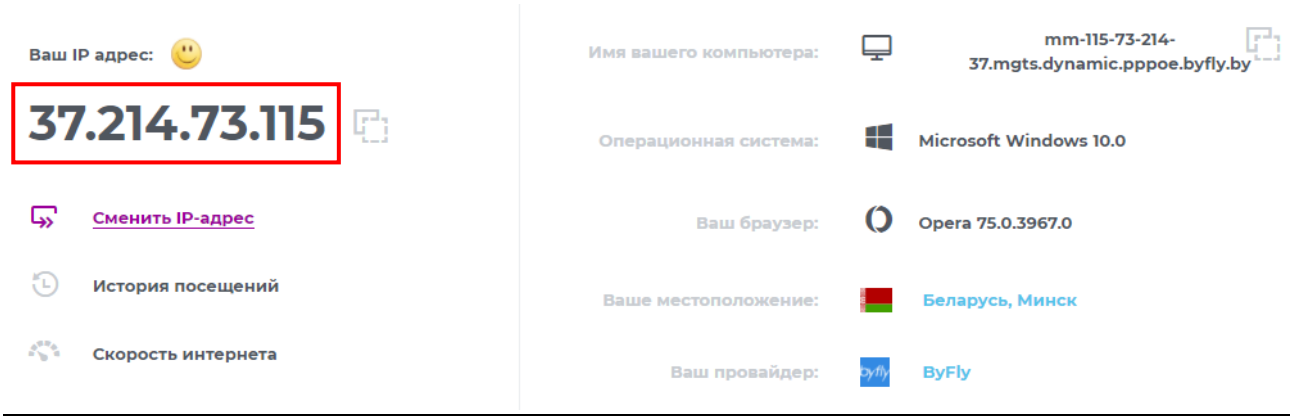
Необходимо понимать, что не всегда внешний IP-адрес является постоянным. Наоборот, IP часто формируется заново от одного подключения к другому.

Б) В зависимости от вариантов определения

Статические. Это IP-адреса, являющиеся неизмененными (постоянными). Они назначаются устройству автоматически в момент его присоединения к компьютерной сети или прописываются пользователем вручную. Статические адреса доступны для использования неограниченное время. Они могут выполнять функцию идентификатора только для одного сетевого узла. Также иногда используется понятие *псевдостатических* адресов, которые работают в пределах одной частной сети.

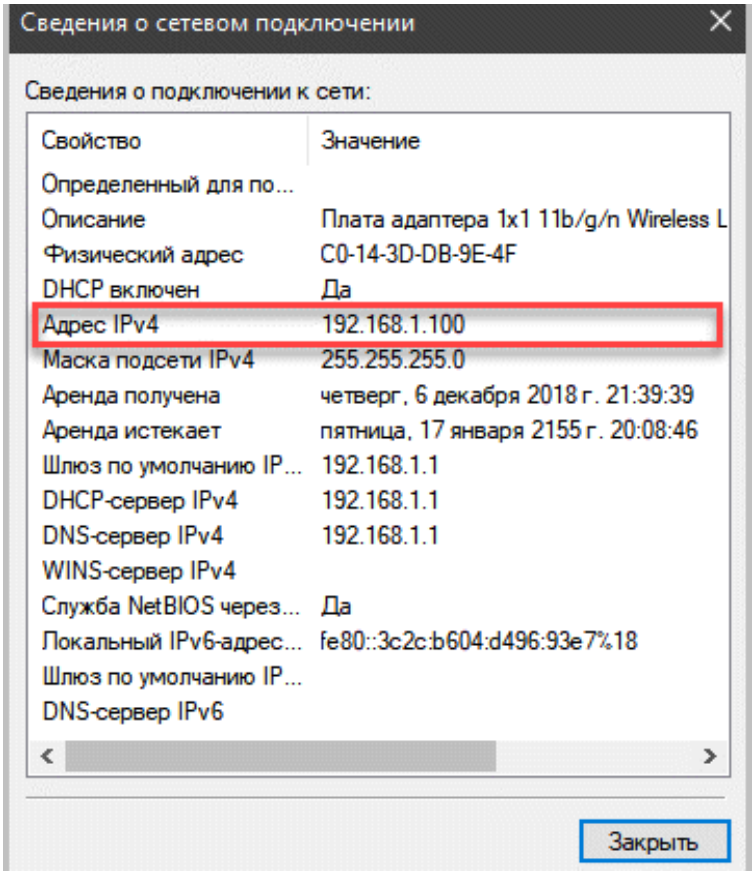
Динамические. Это те IP-адреса, которые выдаются устройству на время. Они автоматически присваиваются в момент подключения к сети и имеют ограниченный срок действия (от начала сессии до ее завершения).

Узнать свой внешний IP-адрес можно с помощью онлайн-сервисов в интернете. Достаточно в поисковой строке «Яндекса» задать запрос «*мой IP*», и нужная информация отобразится в результатах поиска. Также можно воспользоваться сервисом **2ip.ru** (https://2ip.ru), который покажет не только текущий IP компьютера, но и дополнительную информацию о браузере, операционной системе, провайдере, прокси-сервере, местонахождении и других параметрах.



Для того, чтобы просмотреть внутренний IP-адрес, следует выполнить следующую последовательность команд:

Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера → Сетевое подключение → Состояние → Сведения.



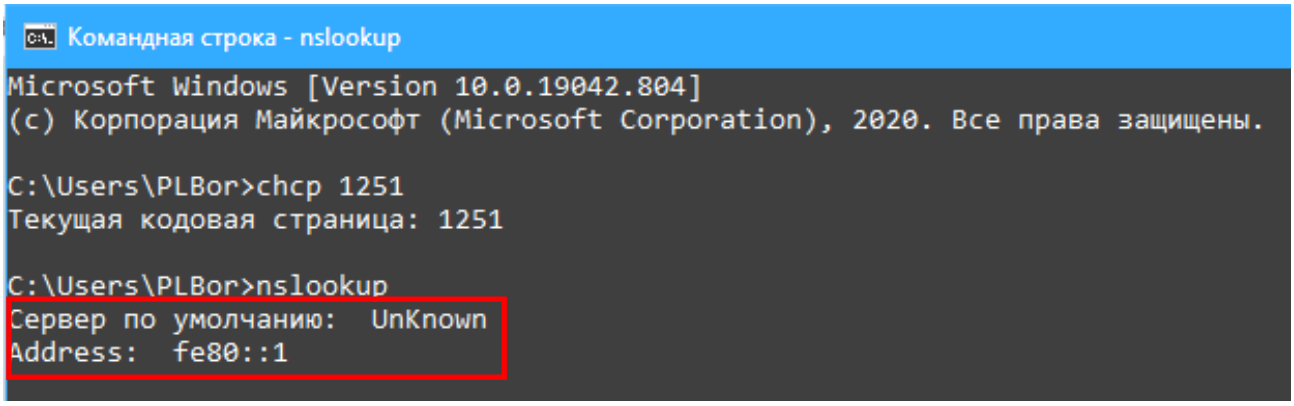
1.2. Символьный адрес DNS

Символьный адрес DNS (англ. Domain Name System «система доменных имён») – компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене.

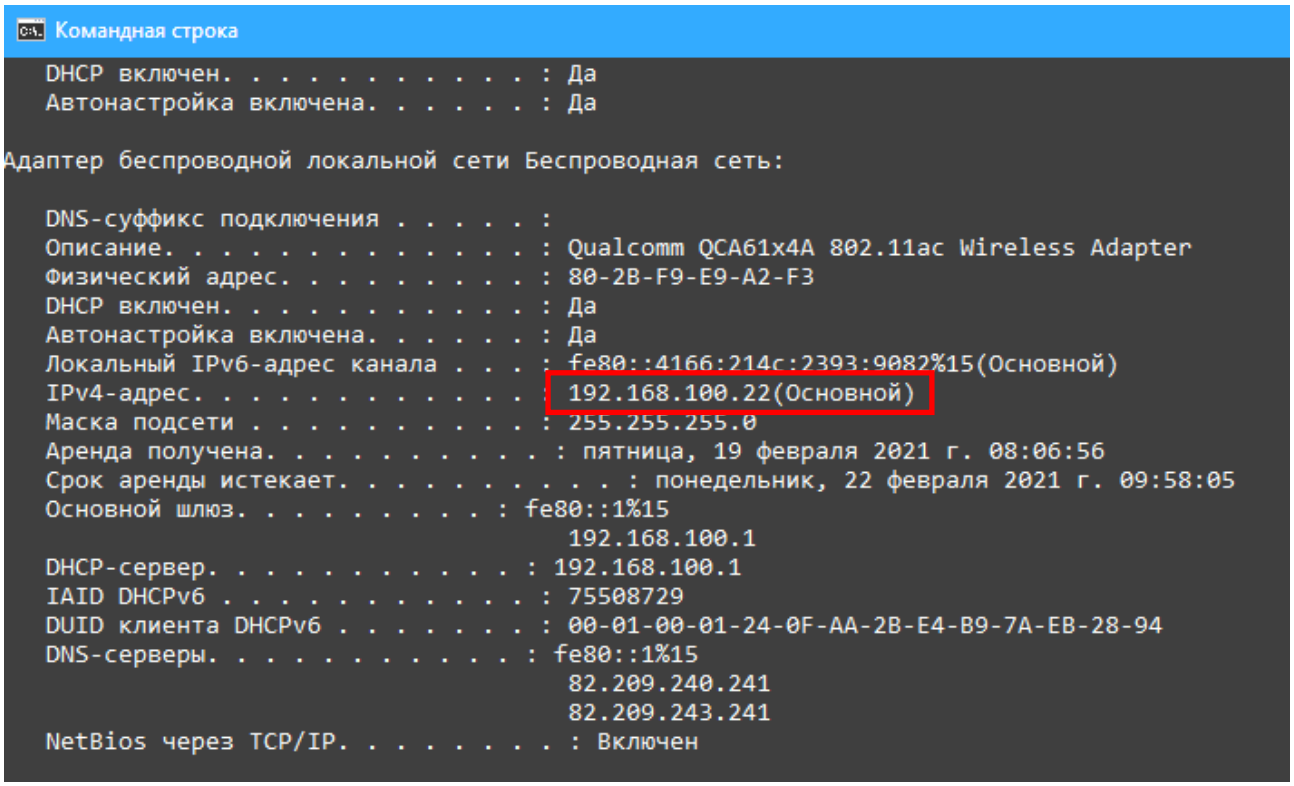
DNS важен для работы Интернета, так как для соединения с узлом необходима информация о его IP-адресе, а для пользователей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса.

Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

Для проверки текущего DNS вы можете воспользоваться встроенной консольной утилитой *nslookup*. Открыв командную строку, выполните в ней сначала команду *chcp 1251*, а затем команду *nslookup*. В результате вы получите название сервера по умолчанию, то есть вашего нового DNS и его адрес, который должен соответствовать предпочитаемому DNS-серверу в свойствах протокола 4 (TCP/IPv4).



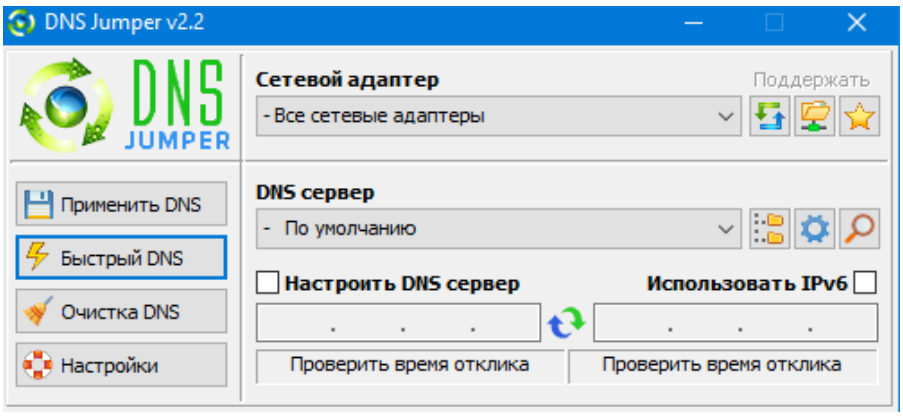
Второй способ – использовать команду *ipconfig/all* в командной строке.



Удобным и альтернативным средством быстрого переключения DNS на ПК для увеличения скорости работы в Интернете или повышения уровня безопасности является портативная и бесплатная программная утилита **DNS_Jumper** (https://www.comss.ru/page.php?id=1749#collapse1).

Основные возможности **DNS_Jumper**:

- Помогает осуществить доступ к заблокированным веб-сайтам;
- Позволяет усилить защиту за счет использования безопасных DNS серверов.
- Позволяет закрыть доступ несовершеннолетних к нежелательным веб-сайтам (за счет использования DNS с родительским контролем).
- Позволяет увеличить скорость веб-серфинга (за счет использования «быстрых» DNS).

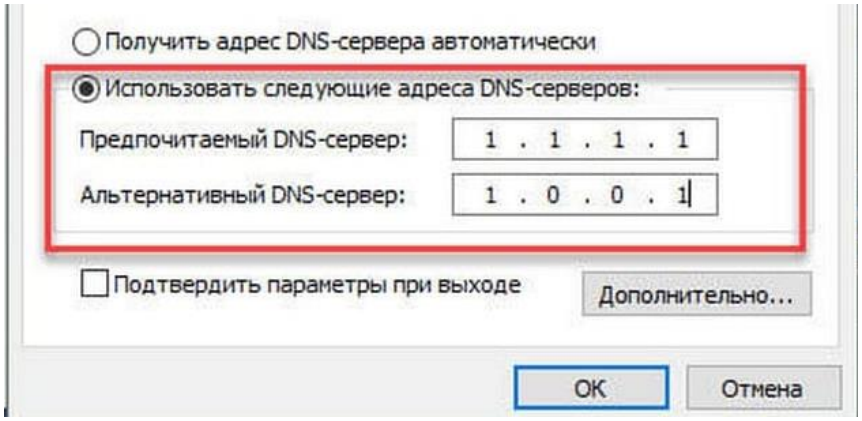


Кроме того, **DNS Jumper** поддерживает создание собственной группы DNS, просмотр текущего DNS и т.д.

Одним из наиболее «быстрых» DNS-каталогов является DNS Cloudflare 1.1.1.1. Независимый тест производительности DNS (https://www.dnsperf.com) показывает, что 1.1.1.1 является самой быстрой службой DNS в мире.

Для того, чтобы установить DNS Cloudflare 1.1.1.1, на странице свойств протокола IP версии 4 (TCP/IPv4) выберите «Использовать следующие адреса DNS-серверов» и введите следующие параметры:

Предпочитаемый DNS-сервер» как 1.1.1.1
Альтернативный DNS-сервер» как 1.0.0.1



Для завершения настройки нажмите «Ок» и перезагрузите браузер.

1.3. MAC-адрес

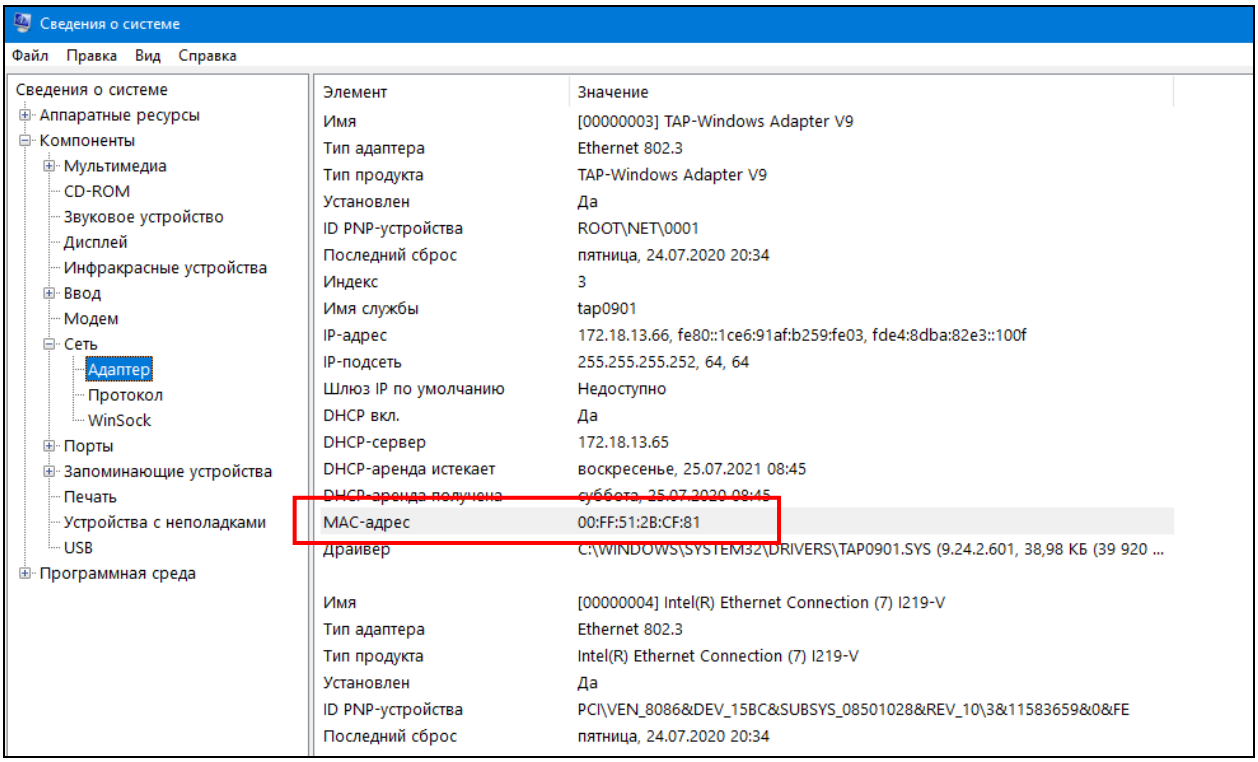
MAC-адрес (от англ. Media Access Control – надзор за доступом к среде, также Hardware Address, также физический адрес) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

Просмотр MAC-адреса в интерфейсе Windows представляет собой следующую последовательность действий:

1. Нажмите клавиши Win+R на клавиатуре, введите *msinfo32*, а затем нажмите Enter.

2. В открывшемся окне «Сведения о системе» перейдите к пункту «Сеть» – «Адаптер».

3. В правой части окна вы увидите сведения обо всех сетевых адаптерах компьютера, включая их MAC-адрес.



Примечание: как правило на ПК установлено две сетевых карты, Ethernet и WiFi, каждый адаптер имеет уникальный MAC-адрес.

Существуют и иные способы установления сведений об IP-адресе, DNS, MAC-адресе.

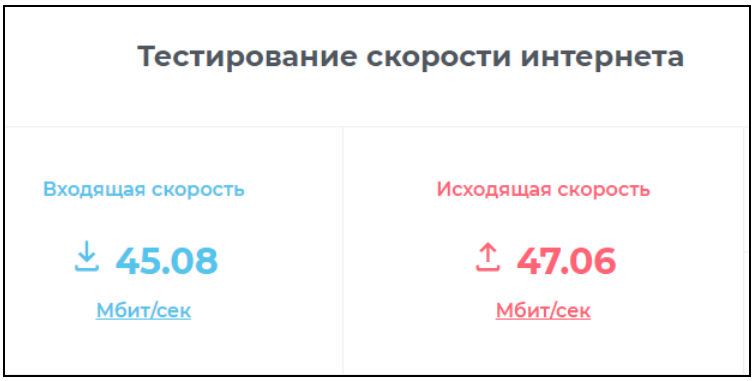
ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (например: «0341 Иванов 4.3»). Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем. При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

1. Ознакомьтесь с теоретическими положениями, изложенными в настоящих рекомендациях и конспекте лекции № 3 «Аппаратное и программное обеспечение защищенных компьютерных систем» данной учебной дисциплины.
2. Выполните просмотр внутреннего и внешнего IP-адресов вашего ПК способами, указанными в теоретической части задания.

Самостоятельно выполните просмотр внутреннего и внешнего IP-адресов вашего ПК иными доступными способами. Результаты зафиксируйте в файл-отчете.

3. Проверьте скорость текущего интернет-соединения с помощью онлайн-сервиса **2ip.ru** (https://2ip.ru/speed/). Результаты зафиксируйте в файл-отчете.



4. Выполните просмотр DNS вашего ПК с помощью команду *ipconfig/all*. Результаты зафиксируйте в файл-отчете.

5. Установите бесплатную программную утилиту **DNS_Jumper** (https://www.comss.ru/page.php?id=1749#collapse1). Изучите ее интерфейс и основные возможности.

5.1. С помощью проверки времени отклика в **DNS_Jumper** осуществите сравнительный анализ наиболее «быстрых» DNS, предлагаемых утилитой. Установите один из них.

С помощью команды *Ping* проверьте время отклика компьютера в сети (интернет-соединение). Для этого в командную строку введите команду:

ping IP_адрес (например, ping 192.168.1.1), либо
ping site -n 10 (например, ping yandex.ru -n 10)

После ввода одной из указанных команд следует нажать Enter.

Результаты зафиксируйте в файл-отчете.

5.2. Проверьте скорость интернет-соединения с помощью онлайн-сервиса **2ip.ru** (https://2ip.ru/speed/). Сравните ее с результатами, полученными при выполнении пункта 3 задания. Результаты зафиксируйте в файл-отчете.

5.3. Восстановите прежние настройки DNS. Для этого нажмите кнопку «Быстрая конфигурация» (имеет значок «Звезда») и выберите «Восстановить настройки DNS» или «Сервер DNS по умолчанию», а затем нажмите кнопку «Применить DNS» в главном окне.

6. Установите DNS Cloudflare 1.1.1.1 способом, указанном в теоретической части задания.

6.1. С помощью команды Ping проверьте время отклика интернет-соединения.

6.2. Проверьте скорость интернет-соединения с помощью онлайн-сервиса **2ip.ru** (https://2ip.ru/speed/).

Сравните ее со значениями, полученными в ходе выполнения пунктов 3 и 5.2 задания. Сформулируйте выводы. Результаты зафиксируйте в файл-отчете.

7. Восстановите прежние настройки DNS.

8. Выполните просмотр MAC-адресов сетевых устройств вашего ПК. Результаты зафиксируйте в файл-отчете.

9. Продемонстрируйте работу и файл-отчет преподавателю.

10. После демонстрации результатов работы преподавателю восстановите исходное состояние системы. Установите первоначальные настройки использованного программного обеспечения.

11. Подготовьте ответ на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что такое сетевой IP-адрес? Типы IP-адресов. Решаемые задачи. Примеры IP-адресов.
2. Перечислите возможные способы установления внутренних и внешних IP-адресов.
3. Что такое символьный адрес DNS? Основное предназначение и решаемые задачи.
4. Перечислите способы проверки и текущего адреса DNS. Установление нового адреса DNS.
5. Охарактеризуйте функциональные возможности бесплатной программной утилиты DNS_Jumper.
6. Перечислите основные возможности DNS Cloudflare 1.1.1.1. Способы установления.
7. Назовите и охарактеризуйте способы проверки скорости текущего интернет-соединения.
8. Что такое MAC-адрес сетевого устройства? Перечислите возможные способы его установления.

2. Способы установления IP-адреса и сведений о нем. Возможности установления личности по IP и MAC–адресам

Краткие теоретические сведения:

1.1. Установление IP-адреса пользователя и сведений о нем

Для получения сведений об организации, предоставляющей доступ к сети Интернет для диапазона IP-адресов, в сети Интернет существует ряд Whois-ресурсов (от англ. «who is» – «кто такой»). Самым популярным среди них является http://centralops.net. Также можно составить запрос вида «whois xxx.xxx.xxx.xxx» (где xxx.xxx.xxx.xxx – искомый IP-адрес) в поисковом сервисе Google.

Среди русскоязычных сервисов наиболее удобными являются http://2ip.ru/, https://whois.ru и др. Если требуется проверить большое количество

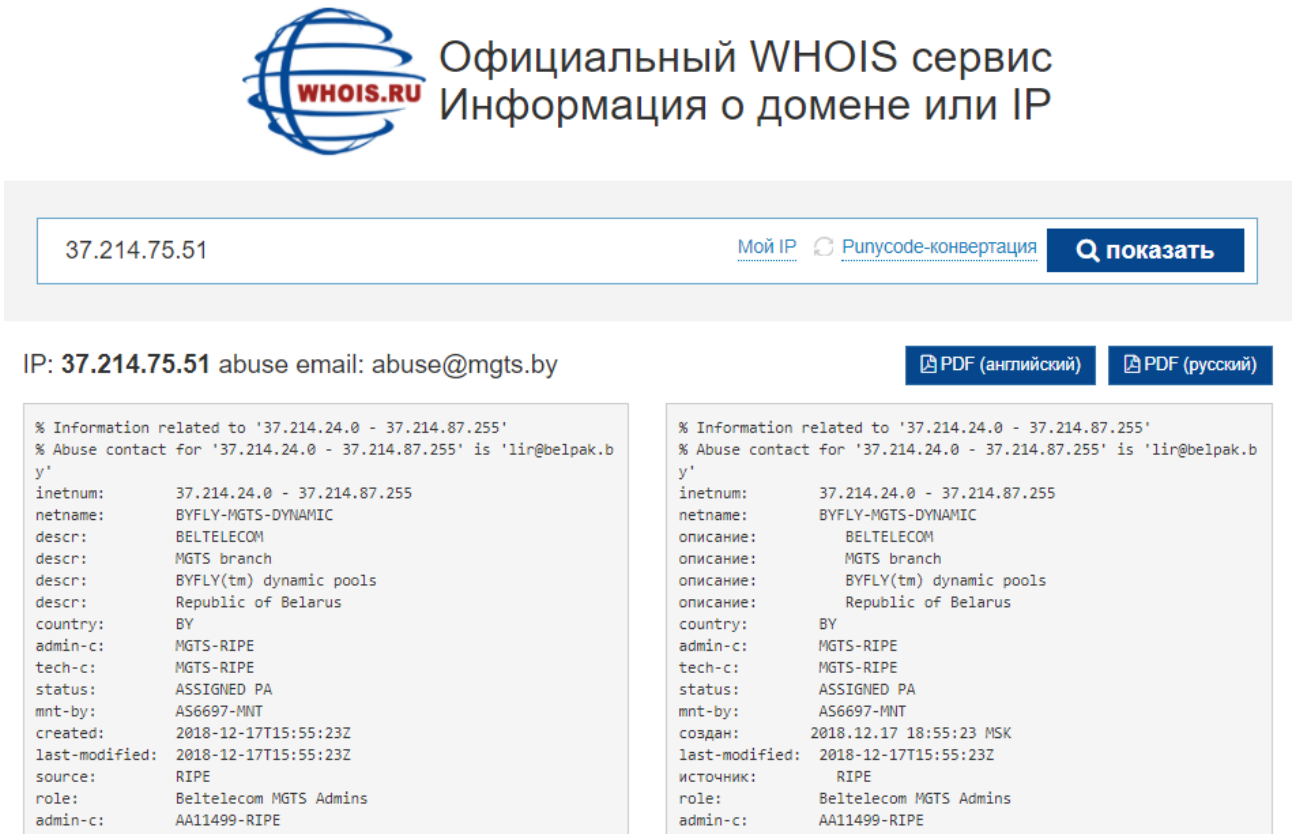
IP-адресов (одним списком), можно воспользоваться онлайн-сервисом http://xseo.in/.

Основная ценность Whois-сервиса в том, что он содержит всю информацию о домене, и обычно позволяет получить данные об истории домена и его владельце. С помощью Whois-сервиса можно выяснить контактные данные владельца домена, дату создания, дату окончания регистрации и многое другое.

При регистрации домена пользователь обязан указать свои фамилию и имя (или, если домен регистрируется на юридическое лицо, – его название), а также почтовый адрес, адрес электронной почты и телефон. По требованию корпорации ICANN, управляющей адресным пространством интернета, введенные контактные данные вносятся в общедоступную базу сведений о зарегистрированных доменах – Whois. Внесение в базу Whois недостоверной информации считается нарушением – доменное имя может быть заблокировано.

Вся эта информация является публичной, однако некоторые регистраторы позволяют скрывать прямые контакты владельца домена. В данном случае будут указаны контакты компании-регистратора.

Следует также учесть, что с помощью Whois-сервиса можно установить лишь название и юридический адрес организации, предоставляющей доступ к сети Интернет для указанного IP-адреса. Для получения сведений о лице, использовавшем искомый IP-адрес в указанное время, необходимо подготовить дополнительный запрос в соответствующую организацию. В том случае, когда организация расположена за пределами Республики Беларусь, необходимо подготовить поручение об оказании правовой помощи.



Официальный WHOIS сервис
Информация о домене или IP

nethouse.ru

Мой IP | Punycode-конвертация | показать

Информация о домене: **nethouse.ru**

Доступен через Брокера | PDF (английский) | PDF (русский)

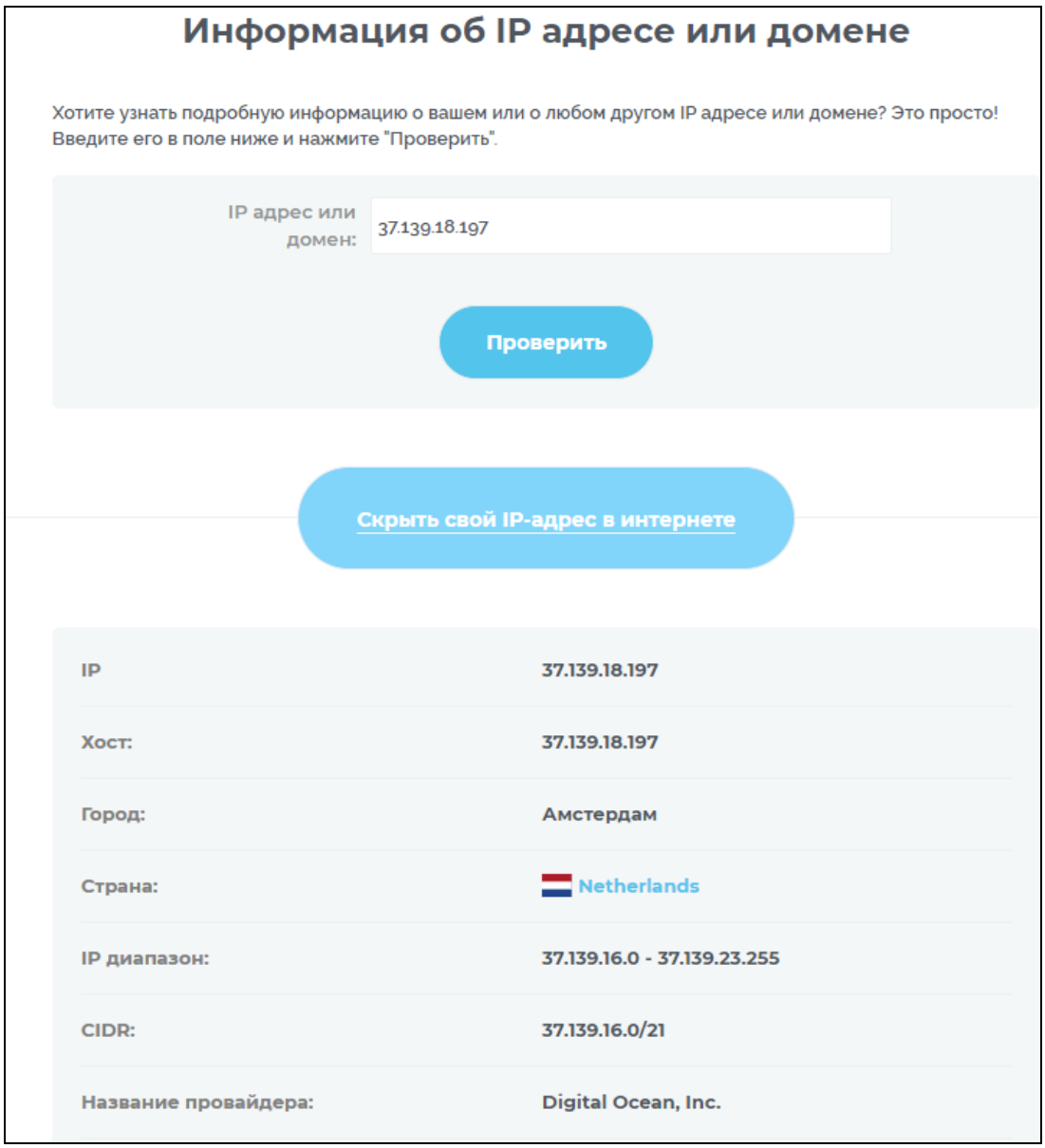
```
domain:         NETHOUSE.RU
nserver:        ns2.majordomo.ru.
nserver:        ns3.majordomo.ru.
nserver:        ns.majordomo.ru.
state:          REGISTERED, DELEGATED, VERIFIED
person:         Private Person
registrar:      NETHOUSE-RU
admin-contact:  https://domains.nethouse.ru/whois/form
created:        2001-03-29T20:00:00Z
paid-till:      2022-04-02T21:00:00Z
free-date:      2022-05-04
source:         TCI
Last updated on 2021-02-20T06:01:48Z
```

```
домен:          NETHOUSE.RU
сервер:         ns2.majordomo.ru.
сервер:         ns3.majordomo.ru.
сервер:         ns.majordomo.ru.
статус:         ЗАРЕГИСТРИРОВАН, ДЕЛЕГИРОВАН, ВЕРИФИЦИРОВАН
владелец:       Private Person
регистратор:    NETHOUSE-RU
форма связи:    https://domains.nethouse.ru/whois/form
создан:         2001.03.30 00:00:00 MSD
оплачен до:     2022.04.03 00:00:00 MSK
дата удаления:  2022.05.04
источник:       TCI
Последнее обновление 2021.02.20 09:01:48 MSK
```

Основные параметры сайта nethouse.ru

- Индекс цитирования: **0**
- Рейтинг Alexa: **29116**
- IP адрес: **185.84.110.41**
- Регистратор домена: **NETHOUSE-RU**
- Дата регистрации: **2001-03-29**
- Дата окончания: **2022-04-02**
- Закончится через: **405 дня**
- Дата проверки: **2021-02-20 05:30:50**

- Внешние ссылки домена: **114**
- Внутренние ссылки: **1**
- Кол-во найденных анкоров: **115**
- Кол-во исходящих анкоров: **114**
- Кол-во ссылок на домене: **115**
- Title страницы: **Конструктор сайтов Nethouse | Создать сайт бесплатно**
- Description страницы: **Создать свой сайт самостоятельно на бесплатном онлайн-конструкторе сайтов Nethouse. Откройте новые возможности для бизнеса - регистрируйся!**
- Keywords страницы: **сайт бесплатно, бесплатный сайт, сделать сайт, конструктор сайтов, создать сайт**



1.2. Установление IP-адреса пользователя, открывшего электронное письмо

Механизм действий по установлению IP-адреса пользователя, открывшего электронное письмо, состоит из следующих операций:

1) Создать ссылку для отслеживания. Для этого следует зайти на https://iplogger.ru (https://iplogger.ru/), нажать кнопку «Невидимый логгер» и сохранить полученную ссылку.

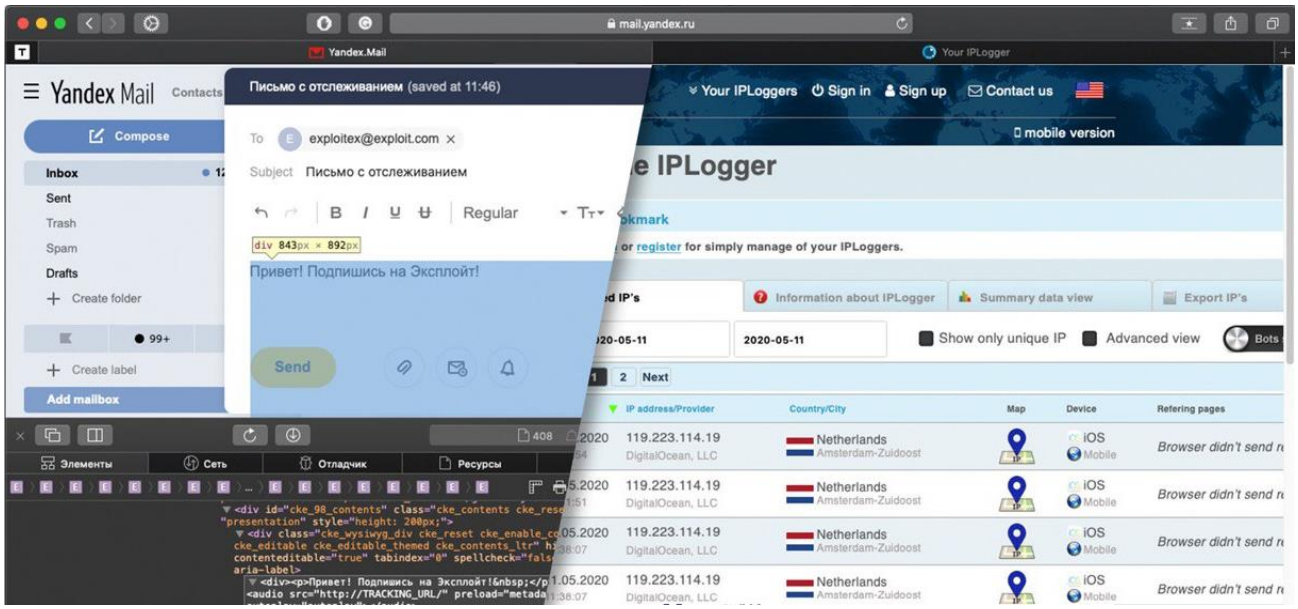
2) Подготовить HTML кода письма (https://pastebin.com/sY8JeD1R), в котором необходимо заменить http://TRACKING URL/ на полученную ссылку из «IPLogger».

3) В поле ввода текста письма следует ввести произвольный текст, а затем нажать правую клавишу мыши и выбрать пункт меню «Просмотреть код».

4) В появившемся окне найти элемент с набранным текстом и выбрать «Edit as HTML». В появившемся блоке необходимо заменить текст на код, предварительно вставив свою ссылку и нажать Ctrl+Enter.

5) Поменять текст письма в самом редакторе и нажать кнопку «Отправить».

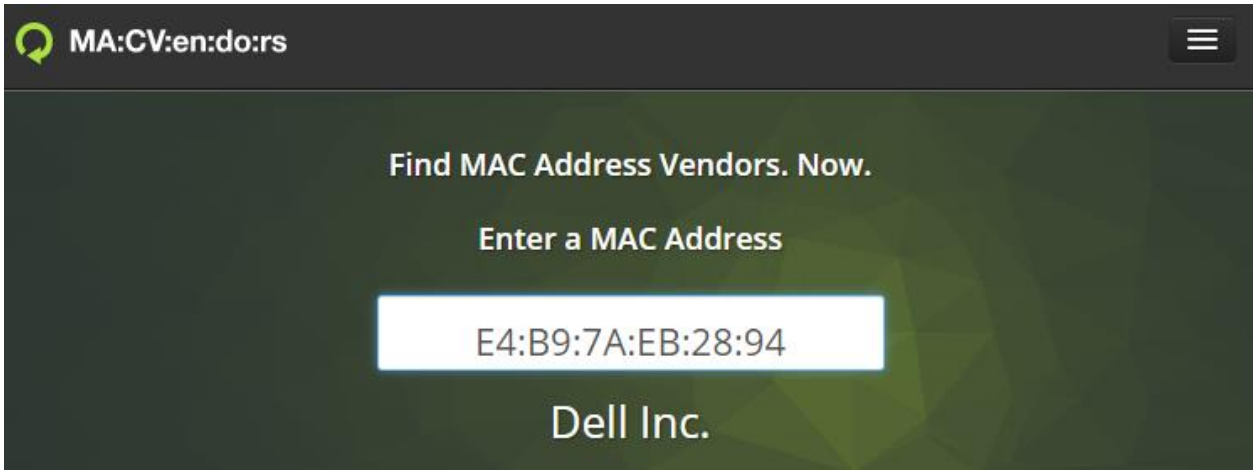
Когда получатель откроет данное письмо, в панели управления логгером появится его IP-адрес.



Данный способ работает не со всеми почтовыми клиентами.

1.3. Установление сведений о сетевом оборудовании по MAC-адресу

Для установления сведений о сетевом оборудовании ПК по известному MAC-адресу рекомендуется воспользоваться одним из онлайн-сервисов, например «Macvendors» (https://macvendors.com/).



Существуют и иные онлайн-сервисы установления сведений о сетевом оборудовании ПК по известному MAC-адресу.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Ознакомьтесь с теоретическими положениями, изложенными в настоящих рекомендациях и конспекте лекции № 3 «Аппаратное и программное обеспечение защищенных компьютерных систем» данной учебной дисциплины.

2. Самостоятельно установите IP-адрес, а также регистрационные сведения о домене следующих интернет-страниц:

http://vkontakte.ru/profile.php?id= 35111967
http://ixbt.com/comm/lan_faq.html
http://www.vgts.ru/doc/tcpip.html
http://www.citforum.ru/nets/ip/contents.shtml
http://www.3com.com/nsc/501302.html

По каждому их полученных результатов сформулируйте выводы. Результаты зафиксируйте в файл-отчете.

3. Выполните просмотр MAC-адресов сетевых устройств вашего ПК. С помощью нескольких онлайн-сервисов установите их принадлежность к определенному виду сетевого оборудования. Результаты зафиксируйте в файл-отчете.

4[1]. Осуществите установление IP-адреса пользователя, открывшего электронное письмо. Для этого с помощью сервиса «iplogger.ru» создайте ссылку для отслеживания, разместите ее в HTML-тексте письма и отправьте по электронной почте. С помощью панели управления логгером установите IP-адрес получателя и удостоверьтесь в его правильности. Результаты зафиксируйте в файл-отчете.

5. Продемонстрируйте работу и файл-отчет преподавателю.

6. Подготовьте ответ на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Основное предназначение Whois-ресурсов. Приведите примеры Whois-ресурсов.

2. Назовите основные функциональные возможности онлайн whois-ресурса «2ip.ru» (http://2ip.ru).

3. Расскажите о механизме действий по установлению IP-адреса пользователя, открывшего электронное письмо

4. Перечислите известные вам онлайн-сервисы по установлению сведений о сетевом оборудовании ПК по известному MAC–адресу.

5. Охарактеризуйте имеющиеся возможности установления личности по IP и MAC–адресам.

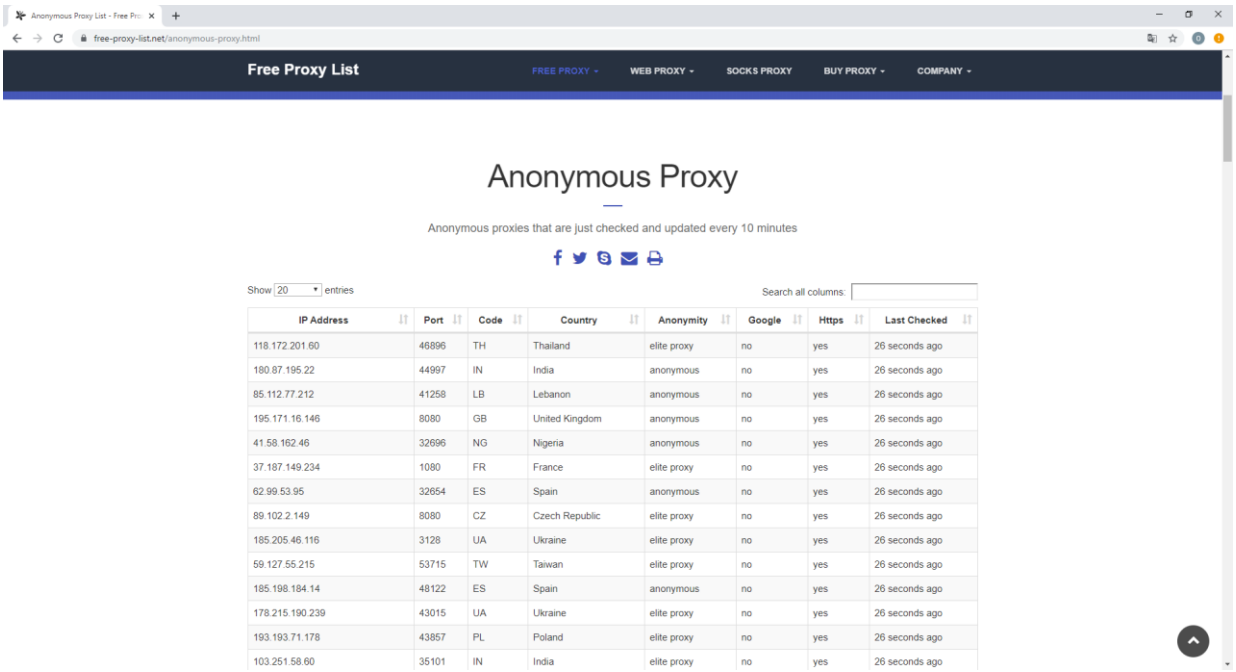
[1] Задание повышенной сложности. Оценивается дополнительно.

3. Использование виртуальных частных сетей (VPN) и прокси-серверов (анонимайзеров) в ходе веб-серфинга

Краткие теоретические сведения:

При проведении регистрации и последующих авторизаций на целевых Интернет-ресурсах для осуществления оперативного поиска в сети Интернет крайне желательно использовать программные решения, предназначенные для подмены конечного IP-адреса пользователя. Подмену IP-адресов конечного пользователя в сети Интернет могут осуществлять сервисы, выступающие в роли «шлюзов», т.е. промежуточным звеном между конечным пользователем и целевым ресурсом.

Такую услугу как на платной, так и на безвозмездной основе предоставляют анонимные «proxy»-серверы.



Для пользования данной услугой достаточно узнать IP-адрес такого сервера (можно получить введя соответсвующий запрос в любой поисковый сервис, например «Google») и внести соотвествующие изменения в настройки используемой программы-браузера. Однако, у этого решения есть весомые минусы: непродолжительность жизни доступных «proxy»-серверов, зачастую низкая пропускная способность (может негативно сказаться на скорости Интернет-соединения) и специальные настройки web-серверов некторых Интернет-ресурсов, запрещающие устанавливать авторизованные соединения с анонимными proxy.

Удобной альтернативой выглядит использование т.н. «виртуальных частных сетей» («Virual Private Networks», или сокращено VPN). VPN создает

защищенный канал связи между вашим компьютером и сервером, и шифрует любые данные, проходящие через него.

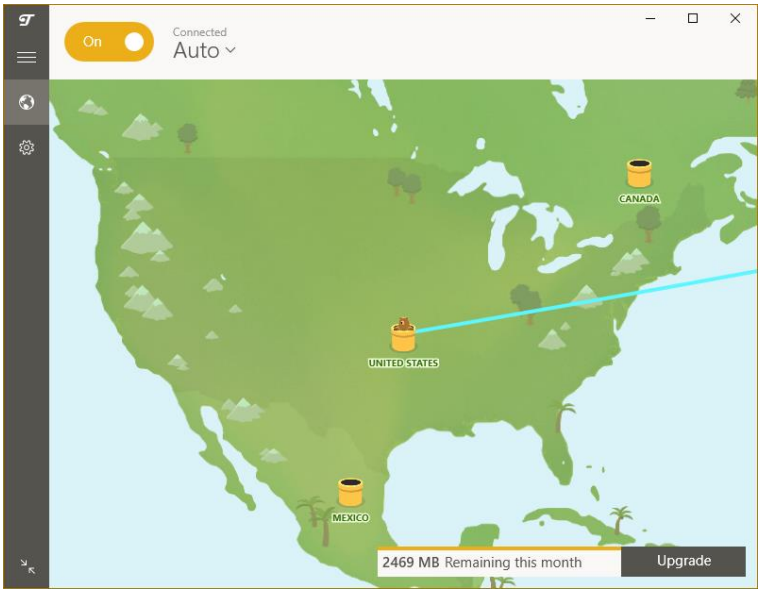
Механизм работы VPN заключается в следующем. Отправленный вами сетевой запрос попадает на сервер ресурса, но ваши данные (информация) могут быть перемещены только между вашим устройством и VPN-сервером, который также проходит по защищенному каналу связи, так что запрашиваемый вами сервер не может получить никакой информации о вас.

При подключении к VPN ваш провайдер не может расшифровать сами данные или отслеживать посещаемые вами веб-сайты, но он может отслеживать только зашифрованный трафик, поступающий на VPN-сервер.

Чаще всего VPN используется для защиты конфиденциальной информации (электронная переписка, интернет-банкинг) и просмотра заблокированных сайтов из любого места. VPN также используется для скрытия реального местоположения путем изменения вашего IP-адреса, который изменяется в зависимости от сервера, к которому вы подключены.

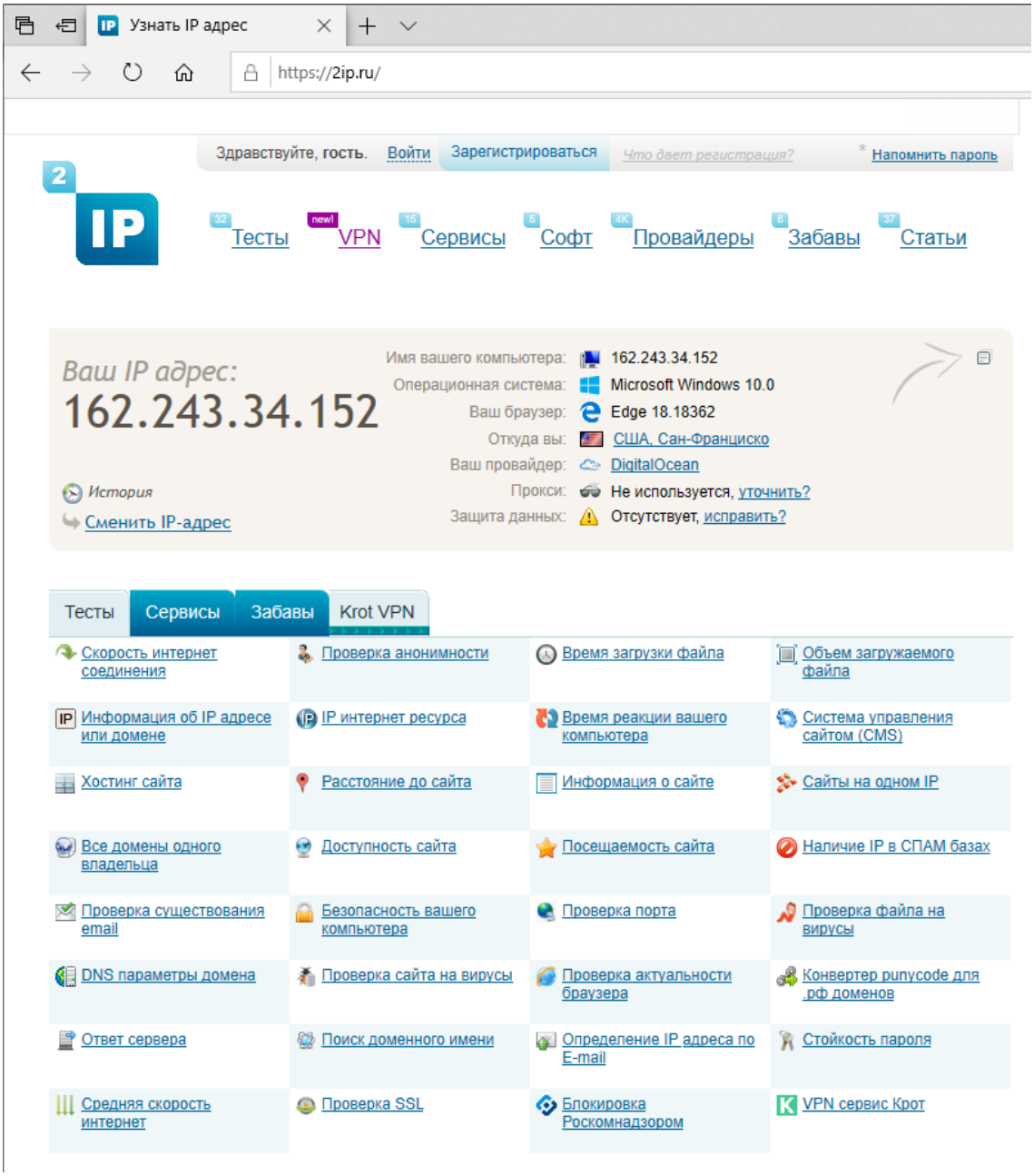
Данные решения предоставляются на платной основе, и зачастую требуют внесения изменений в настройки сетевого подключения используемой операционной системы.

Эксплуатацию VPN упрощает приложение «Tunnel Bear» (https://www.tunnelbear.com). Оно является оптимальным, в случаях когда передаваемый анонимным способом сетевой траффик (т.е. информаиця передаваемая по сети) не велик по объему. Приложение предусматривает как платную, так и бесплатную подписку для зарегистрированных пользователей. Бесплатная подписка подразумевает 500 Мб анонимного траффика в месяц, причем в случае его неиспользования, трафик суммируется с вновь получаемым в новом месяце. Программа проста в использовании – приложение само устанавливает VPN-соединение по нажатию на одну кнопку. Пользователю необходимо лишь выбрать страну – место размещения сервера.



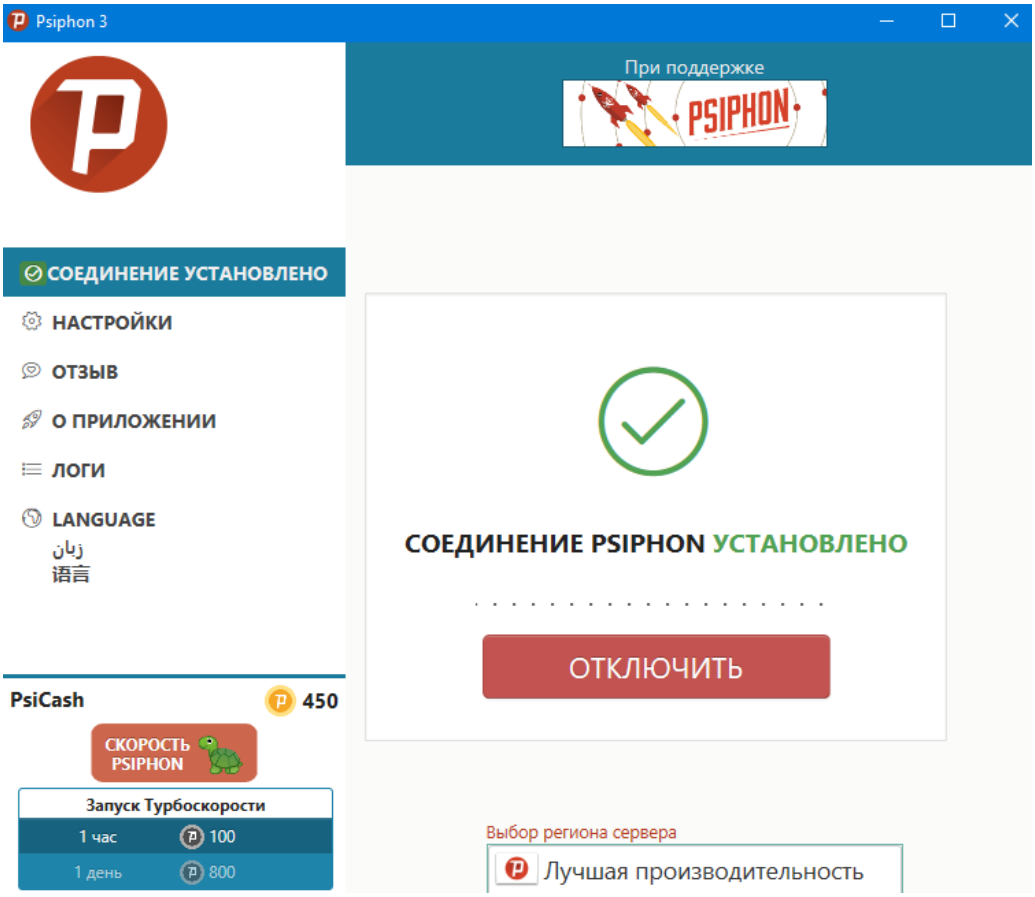
Приложение реализовано на платформах операционных систем семейства «Micorosft Windos», «Linux», «Android», «macOS», «iOS».

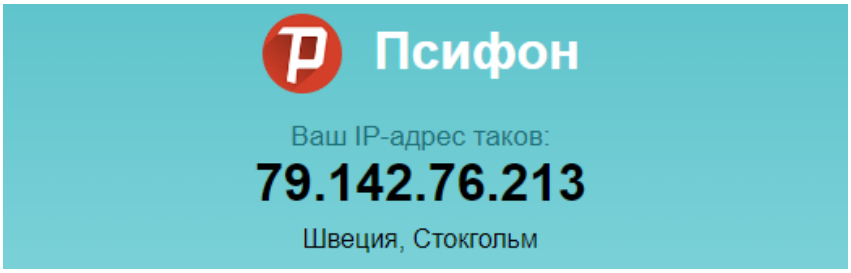
После установки и настройки программного обеспечения, его работоспособность можно проверить посещением Интернет-сайта, отображающего текущий IP-адрес посетителя (например, «2ip.ru»).



Следующим альтернативным средством VPN является программа Psiphon (https://www.psiphon3.com/ru/download.html). Это бесплатный инструмент с открытым исходным кодом, в котором используется сочетание технологий защищенной связи и обфускации. Psiphon – это централизованно управляемая и географически разнородная сеть из тысяч прокси-серверов, использующая

ориентированную на производительность архитектуру с одним или несколькими переходами.





Существуют и иные программные средства, предназначенные для подмены конечного IP-адреса пользователя.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Ознакомьтесь с теоретическими положениями, изложенными в настоящих рекомендациях и конспекте лекции № 3 «Аппаратное и программное обеспечение защищенных компьютерных систем» данной учебной дисциплины.
2. Выполните просмотр внешнего IP-адреса вашего ПК. Результат зафиксируйте в файл-отчете.

3. Скачайте с официального сайта, установите и настройте приложение «Tunnel Bear» (https://www.tunnelbear.com). Выполните его запуск.

3.1. Удостоверьтесь в подмене своего IP-адреса. Результат зафиксируйте в файл-отчете.

3.2. Удалите программу «Tunnel Bear» с вашего ПК.

4. С помощью открытых ресурсов сети Интернет осуществите поиск, установку и настройку иных программных средств (например, Psiphon (https://www.psiphon3.com/ru/download.html), либо онлайн-сервисов, предоставляющих бесплатные услуги VPN (например, https://www.freeopenvpn.org/). Удостоверьтесь в их работоспособности.

Сравните результаты их работы (скорость работы, устойчивость интернет-соединения, географическое расположения серверов и др.). Результаты зафиксируйте в файл-отчете.

5. Продемонстрируйте работу и файл-отчет преподавателю.

6. После демонстрации результатов работы преподавателю восстановите исходное состояние системы (удалите установленные программы). Установите первоначальные настройки использованного программного обеспечения.

7. Подготовьте ответ на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Виртуальные частные сети (VPN): сущность, предназначение, направления использования в служебной деятельности. Приведите примеры известным вам сервисов VPN.
2. Прокси-сервер: понятие и сущность. Основные направления использования. Чем отличается от VPN? Приведите примеры известных вам прокси-серверов.
3. Виды VPN. Отличия и особенности. Приведите примеры.
4. Возможности деанонимизации пользователей VPN.
5. Потенциальные угрозы, возникающие при использовании VPN.

4. Составление запросов операторам электросвязи на получение информации

Краткие теоретические сведения:

Если в ходе раскрытия либо расследования киберпреступления будет установлен IP-адрес, с использованием которого осуществлена регистрация электронного кошелька, в последующем перемещались денежные средства, а также осуществлялся доступ в сеть Интернет с использованием мобильного телефона, необходимо подготовить запрос в организацию, предоставляющую доступ к сети для указанного диапазона IP -адресов.

Если это внутренняя сеть общего пользования, то для составления запроса достаточно просто установить организацию, предоставляющую к ней доступ. В случаях размещения информации в сети Интернет установить организацию, предоставляющую доступ с указанного IP-адреса, не всегда возможно (это может быть публичный адрес гостиницы или интернет-кафе).

На территории Республики Беларусь в рамках Указа Президента Республики Беларусь от 01 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет», любая организация, предоставляющая доступ к сети Интернет (в том числе почта, клубы, кафе, гостиницы), с 01 июля 2010 г. обязана хранить полные сведения о фактах подключения не менее одного года.

При составлении запросов в обязательном порядке необходимо ссылаться на конкретные статьи нормативно-правовых актов Республики Беларусь.

Примерный перечень сведений, запрашиваемых у интернет-провайдеров *(на примере РУП «Белтелеком»)**:***

1. полную информацию (*имя аккаунта, его принадлежность, номер исходящего телефона; при наличии договора о предоставлении услуг выхода в сеть Интернет – сведения о лице, заключившем договор, дату и срок действия договора, MAC-адрес устройства, с которого осуществлялся выход в сеть Интернет*) по следующему примерному соединению:

IP-адрес	дата	время	посещаемый интернет-ресурс (диапазон IP-адресов)
93.85.150.56	20.07.2016	с 15.30 по 14.40	«bps-sberbank.by»

2. информацию о телефонных абонентских номерах, с которых осуществлялся выход в сеть Интернет под логином **********@beltel.by, принадлежащим по договору об оказании услуг электросвязи № ********** от **.**.20** гражданину *(Ф.И.О.)*, в период времени с **.**.20** по **.**.20**;

3. сведения:

- обо всех входах в сеть Интернет, с указанием используемого логина, даты и времени входа с сетевого устройства, имеющего MAC-адрес: *CC:7B:35:17:17:B9* в период времени с **.**.20** по настоящее время;

- об абонентах РУП «Белтелеком», логины которых использовались для входа в сеть Интернет с указанного сетевого устройства в указанный период времени;

4. об IP-адресах доступа к кабинету пользователя **********@beltel.by, с которых осуществлялась смена пароля в период времени с **.**.20** по **.**.20** с указанием даты и время доступа;

5. историю посещения абонентом (договор № ********** от **.**.20**) информационных ресурсов в период времени с **.**.20** по настоящее время с

указанием MAC-адреса устройства и телефонного абонентского номера, адреса с которого осуществлялся выход в сеть Интернет;

6. обо всех входах в сеть Интернет с сетевого устройства, имеющего MAC-адрес: **:**:**:**:**:**, с указанием данных абонента, заключившего договор, дату и срок действия договора, телефонного абонентского номера, адрес с которого осуществлялся выход в сеть Интернет в период времени с **.**.20** по настоящее время.

Примерный перечень сведений, запрашиваемых в организациях, осуществляющих хостинг и обслуживание интернет-ресурсов:

1. сведения обо всех доступах, в том числе неудачных попытках, к сетевым ресурсам «www.**********.by» в период времени с 01.01.2013 по настоящее время;

2. отчеты о проделанной работе сотрудниками УП «Надежные программы» по восстановлению удаленной информации и настройке доступа к сетевым ресурсам «www.**********.by» в период времени с **.**.20** по настоящее время;

3. журналы доступа к интернет-ресурсу «www.********.by», в том числе к административной панели, FTP и базам данных за максимально возможный период времени;

4. время хранения резервных копий файлов указанного интернет-ресурса, а также резервных копий баз данных.

Примерный перечень сведений, запрашиваемых в финансовых организациях:

1. по банковскому счету:

- регистрационные данные лица, указанные при открытии счета;
- движение денежных средств с момента открытия счета по настоящее время (с указанием даты, времени, назначения платежей, переводов и иных возможных операций);
- данные всех БПК эмитированных к счету;
- IP-адреса доступа к Интернет-банкингу с момента регистрации счета по настоящее время.

2. по банковской платежной карте:

- информацию об операциях, с использованием БПК № ********** в период времени с **.**.20** по **.**.20** с указанием даты, времени, места (страна, город), полных сведений о точке (интернет, банкомат, магазин, название обслуживающего банка) проведения операции, вида операции (оплата услуг, покупка товара, снятие наличных), суммы денежных средств, типа транзакции, результата операции.

3. в отношении электронных кошельков:

- данные, указанные лицом при регистрации;
- IP-адреса входов и выходов в учетную запись кошелька;
- сведения об операциях, совершенных с использованием всех имеющихся электронных кошельков, прикрепленных к идентификатору

пользователя за максимально возможный период времени *(можно указать конкретный период времени, например: в период времени с 00:00 часов 21.03.2017 по 24:00 часа 23.03.2017)*.

Необходимо отметить, что указанный перечень не является исчерпывающим и зависит от конкретной ситуации.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Ознакомьтесь с теоретическими положениями, изложенными в настоящих рекомендациях и конспекте лекции № 3 «Аппаратное и программное обеспечение защищенных компьютерных систем» данной учебной дисциплины.
2. Подготовить письмо в адрес начальника Управления по противодействию преступлениям в сфере высоких технологий Министерства внутренних дел Республики Беларусь с просьбой об оказании содействия в получении информации об IP-адресах компьютера, с которого осуществлялась регистрация пользователя и доступа к странице http://vkontakte.ru/profile.php?id=35111967 на интернет-сайте www.vkontakte.ru, номера ID, электронной почты, номера мобильного телефона, с указанием даты и времени ввода информации.
3. Подготовить письмо на имя директора Минского филиала РУП «Белтелеком» с просьбой о предоставлении полной справочной информации (имя аккаунта, его принадлежность, номер исходящего телефона; при наличии договора о предоставлении услуг выхода в сеть Интернет – сведения о лице, заключившем договор, дату и срок действия договора) по следующим соединениям:

IP-адрес	Дата	Время минское
86.57.129.96	07.04.2020	14:46
93.84.99.86	11.04.2020	21:08

4. Продемонстрируйте работу преподавателю.

5. Подготовьте ответ на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Какой нормативные правовой акт Республики Беларусь устанавливает требования для организаций, предоставляющих доступ к сети Интернет, хранить полные сведения о фактах подключения не менее одного года?
2. На какие конкретные статьи нормативно-правовых актов Республики Беларусь в обязательном порядке необходимо ссылаться при составлении запросов для установления IP-адреса, с использованием которого осуществлена регистрация электронного кошелька, перемещались денежные средства, либо осуществлялся доступ в сеть Интернет?

3. Опишите примерный перечень сведений, запрашиваемых у интернет-провайдеров (на примере РУП «Белтелеком»).

4. Опишите примерный перечень сведений, запрашиваемых в организациях, осуществляющих хостинг и обслуживание интернет-ресурсов.