ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Дисциплина:

«Основы кибербезопасности»

ОТЧЕТЫ ПО ЛАБОРАТОРНО-ПРАКТИЧЕСКИМ РАБОТАМ

Выполнил:

Величко Максим Иванович

Поток 1.3

гр. M32061, 334786

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*



(подпись)

Проверил:

Власов В.В.

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Санкт-Петербург

2022

**Практическая работа №1: «Цифровые следы в Интернете и основы социальной инженерии».**

Предмет исследования – вы сами. Проанализируйте ваше присутствие в Интернете. Найдите свои профили в социальных сетях, мессенджерах, сайтах, приложениях через поисковые системы. Используйте данные о вас, которые могут быть раскрыты вами намеренно или непреднамеренно. Ответьте на следующие вопросы (учитывайте, что данный файл будет доступен другим пользователем общей папки, куда вы загружаете его, поэтому не пишите тут ваши пароли и иную чувствительную информацию о вас):

1. Какие инструменты вы использовали для анализа ваших цифровых следов? Опишите работу с ними.

|  |
| --- |
| Для анализа моих цифровых следов я использовал поисковые системы, такие как Google, Yandex. Я вводил мое имя и фамилию в поисковую строку и просматривал выдачу результатов для поиска моих профилей в социальных сетях, мессенджерах, сайтах и приложениях. Я также использовал поисковые запросы для поиска сведений обо мне, которые могут быть доступны другим пользователям. |

1. Оцените по 5 бальной шкале насколько безопасно вы ведете себя в интернете, заполните таблицу:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Вопрос** | **Ваша оценка**  *1-плохо, небезопасно,*  *5 – очень хорошо, высокий уровень безопасности* | **Объясните почему именно такую оценку вы поставили** |
| 1 | Обо мне можно найти информацию в Интернете | 4 | Данные о месте учебы и то, чем я занимаюсь публично могут найти в интернете. Но данные о личной жизни или какую-то подробную информацию не найти |
| 2 | По информации в интернете и социальных сетях можно узнать, где я работаю/учусь, кто мои друзья и какие у меня интересы | 3 | Можно найти место учебы и предположить кто мои друзья. |
| 3 | Я зарегистрирован в более чем двух социальных сетях  *Чем больше соцсетей, тем больше цифровых следов* | 3 | ВК, Facebook, Twitter, Instagram |
| 4 | Я использую социальные сети и мессенджеры безопасно  *Оцените самостоятельно, в том числе открытый ли у вас профиль и пр., ваше полное отсутствие в соцсетях соответствует высокому уровню безопасности,* | 3 | Мои профили являются открытыми |
| 5 | Меня можно найти в социальных сетях и мессенджерах по номеру телефона *Чем проще это сделать – тем ниже оценка, 5 – найти нельзя* | 5 | Данную информацию я скрываю |
| 6 | Я использую сложные пароли в критических для меня приложениях и сайтах (почта, социальные сети, мессенджеры и прочее). *Пароли разные? Очень сложные? Чем больше правил вы соблюдаете – тем выше оценка.* | 5 | Да, я использую защищенное хранилище для паролей с шифрованием и автоматической генерацией. |
| 7 | Я внимательно отношусь к тому, по каким ссылкам хожу в интернете | 5 | Да. Использую только проверенные ресурсы |
| 8 | Насколько вы активны в соц.сетях *Постинг, сторис, комментирование, создание контента  прочее* | 4 | Практически ничего не комментирую. Создаю немного контента, в основном, в Telegram. |
| 9 | Мой компьютер защищен от вирусов | 4 | Использую антивирус. |
| 10 | Регулярно обновляю программное обеспечение, не устанавливаю пиратское и взломанное ПО, знаю где найти номер последней версии браузера, операционной системы на десктопе или телефоне | 4 | Стараюсь обновлять ПО регулярно. Автоматическое обновление работает постоянно. |
| 11 | Я сижу в даркнете  *Дайте самостоятельную оценку по вашим личным критериям данного пункта* | 1 | Нет. Я не сижу в Даркнете. |
| 12 | Я использую VPN, tor, proxy | 5 | Использую проверенные VPN, которые не сливают особо информацию. |
| 13 | Я использую менеджеры паролей | 5 | Конечно. |
| 14 | Я предпринял меры, чтобы не потерять ценную информацию с компьютера/телефона | 5 | Конечно. |
| 15 | Оцените как часто вы делаете покупки в интернете и оставляете данные вашей карты | 4 | Карту не сохраняю. |
| 16 | Вы активно интересуетесь службами шифрования, наличием многофакторной аутентификации у сервисов, которые используете и подключаете их при наличии | 5 | Да. Если сервис для меня важен, то я подключаю многофакторную аутенфикацию. |
| 17 | Вы подошли ответственно к выбору сервиса почтовой службы (предпочитаете использовать gmail.com вместо mail.ru, например), к выбору мессенджера (отдаете предпочтение безопасным  Signal, Telegram вместо Whatsapp), а также иным поставщикам онлайн сервисов | 5 | Конечно! Telegram |
| 18 | Оцените в целом вашу стратегию (и есть ли она вообще) безопасного присутствия в Интернете и того, как вы работаете со своим цифровым следом | 4 | Минимум информации о чем-то личном. Использование стандартных методов, которым желательно пользоваться всем - защищенный менеджер паролей, антивирус и т.п. |

1. Какие выводы вы сделали и что нужно изменить в вашем поведении в социальных сетях, чтобы уменьшить риск использования против вас методов социальной инженерии с целью обмана вас, получения информации от вас или использования вас в каких-либо противоправных действиях в отношении вас, компании в которой вы работаете или людей, которых можете знать:

|  |
| --- |
| Думаю, что при текущих объемах сбора информации и слива рекламодателям (и не только!) полностью нельзя убрать цифровой след, но можно постараться меньше его оставлять. Я считаю, что я хорошо осведомлен о базовых средствах и методах защиты, чтобы меня можно было провести (нужно быть всегда начеку). |

**Лабораторная работа №1: «Заражение вирусом»**

1. Параметры операционной системы:

Выпуск Windows 11 Домашняя для одного языка

Версия 21H2

Дата установки ‎24.‎10.‎2021

Сборка ОС 22000.1335

Взаимодействие Windows Feature Experience Pack 1000.22000.1335.0

2.

Изображение выглядит как текст

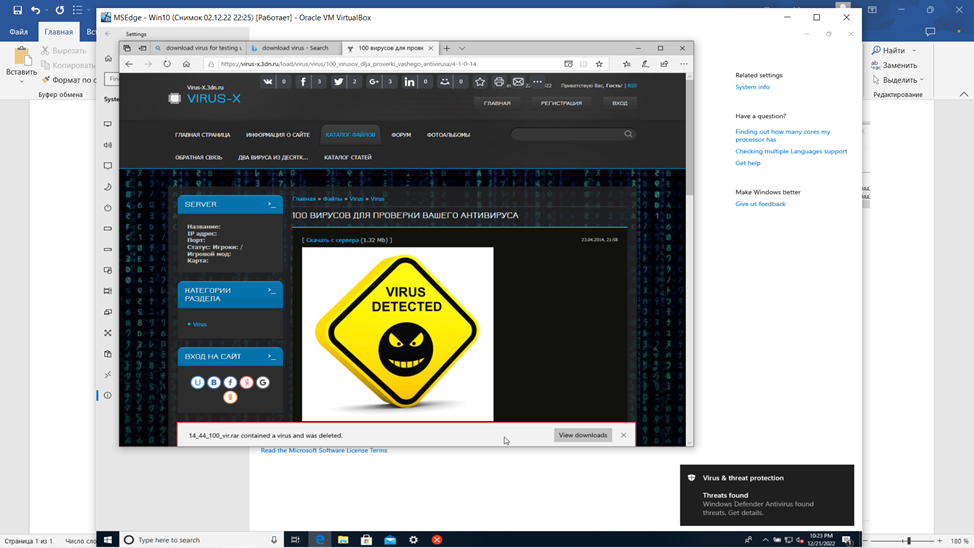
Автоматически созданное описание

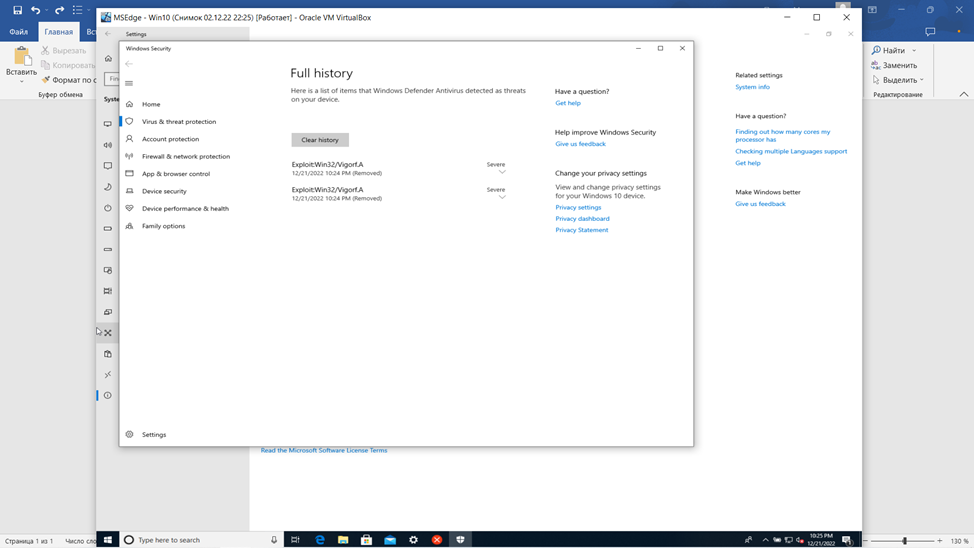
3. Параметры виртуальной операционной системы, которую я поставил:

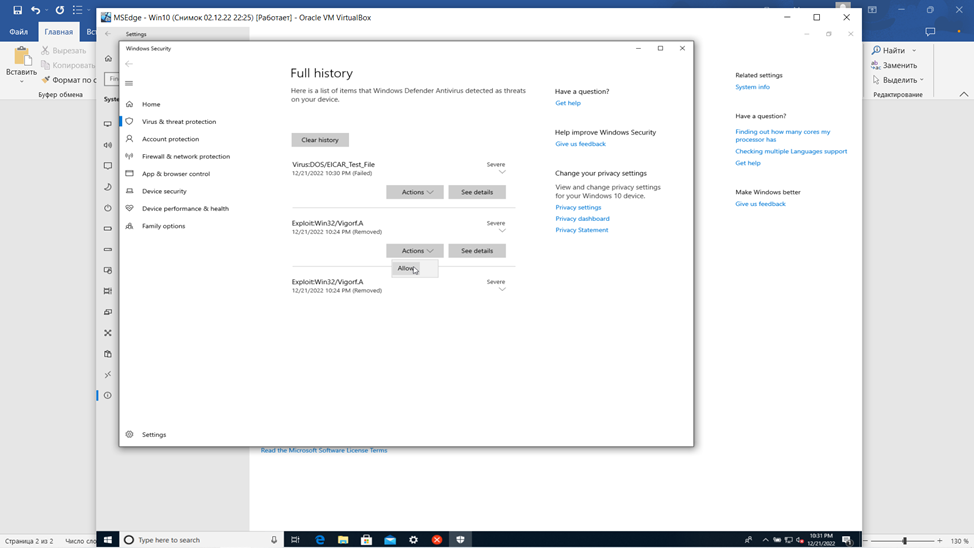
Изображение выглядит как текст

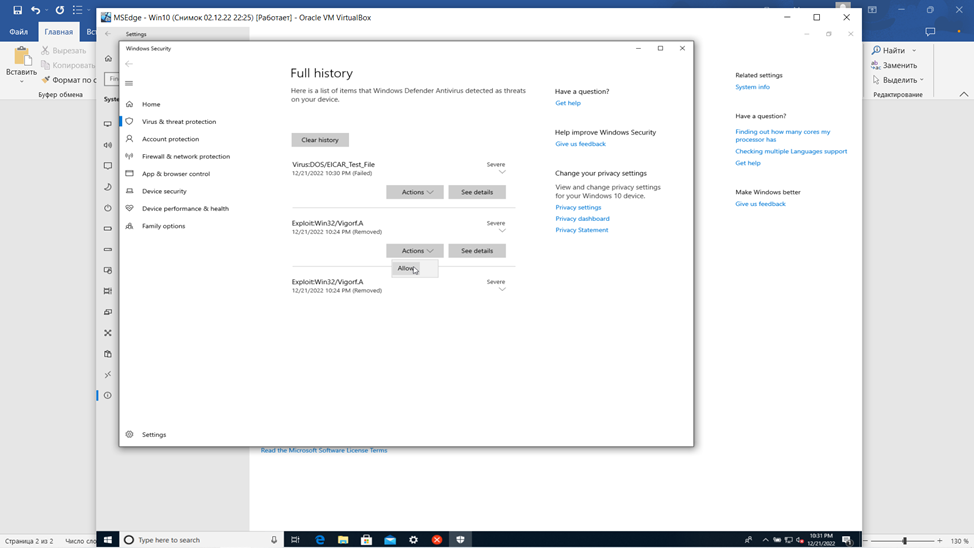
Автоматически созданное описание

1. В виртуальной windows скачал и запустил вирус:









После запуска вируса экран стал зависать, компьютер начал шуметь. Курсор практически не двигался - двигался рывками через достаточно большие промежутки времени (пример так, как когда открываешь штук 10 вкладок в Сhrome)

Размер свободной оперативной памяти уменьшился, стали появляться странные файлы. Диск и нагрузка на видеокарту была загружена на 95%

Перезагрузка компьютера не помогла.

Я попробовал закрыть все процессы копирования файлов и отключить приложения в автозагрузке. Это помогло, но не до конца. Компьютер всё ещё зависал. Были все те же процессы, которые остались после перезагрузки, которые закрыть не удалось.

Тогда я запустил антивирус и удалил вредоносное ПО, исправил все неполадки. После перезагрузки Windows все стало работать нормально.

1. Выводы по работе.

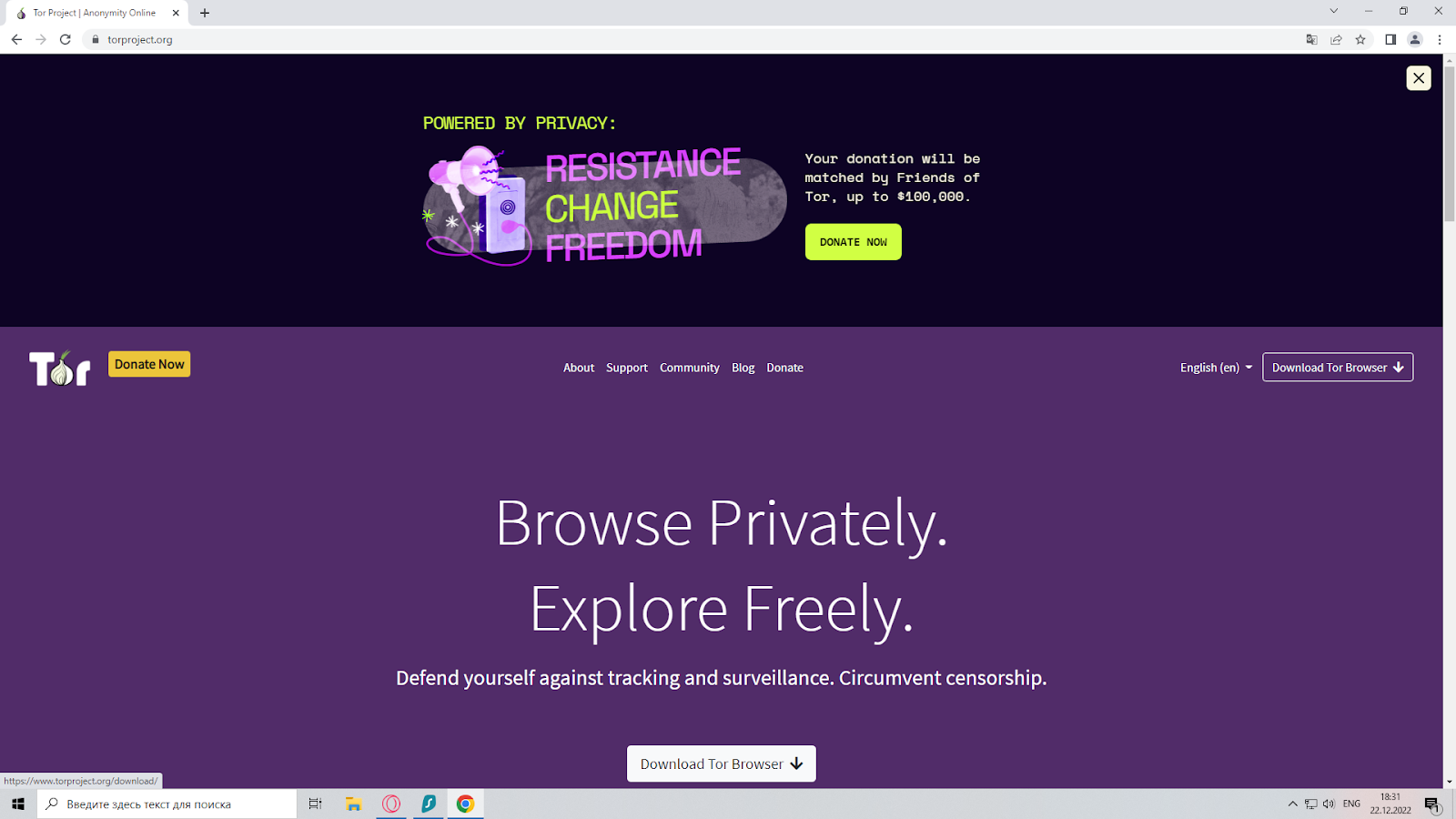
Компьютерные вирусы и вредоносные программы очень опасны как для компьютера и данных, хранящихся на нём, так и для самого человека, который не хочет распространения этих данных. Вирусы могут не только замедлить работу устройства, но и воровать данные или вообще сломать всю систему, повредив системные файлы.

Чтобы уменьшить вероятность заражения вирусом компьютера нужно использовать хорошие антивирусы, регулярно делать проверку.

Компьютерные вирусы на самом деле очень опасны и могут не только замедлить работу компьютера, но и повредить системные файлы, что приведет к невозможности загрузки ОС. Поэтому нужно пользоваться антивирусом и с умом скачивать что-либо из Интернета.

**Лабораторная работа №3: «Использование браузера TOR»**

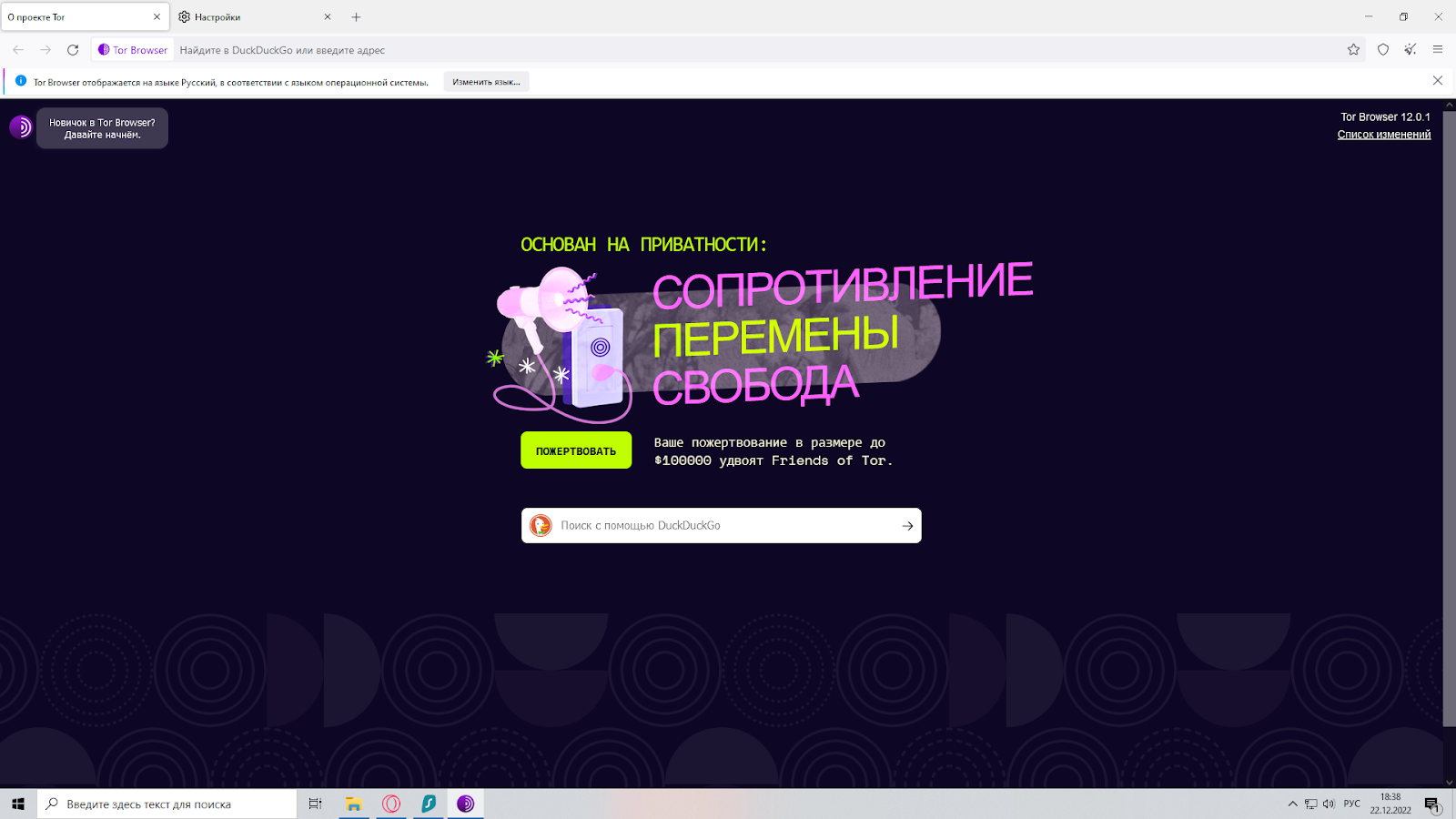
1. Устанавливаем браузер, все на той же виртуальной системе



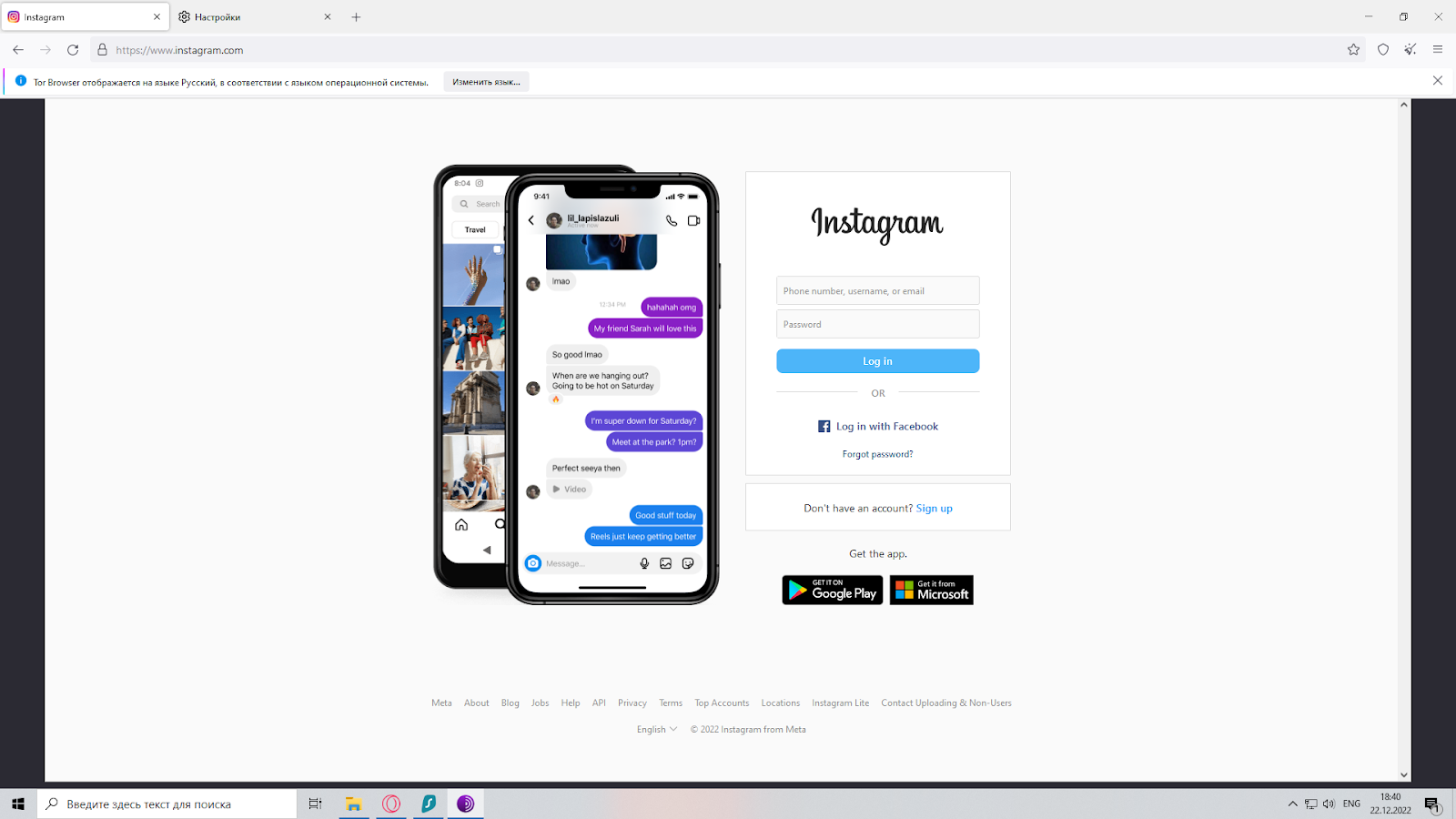
Пришлось скачать и открыть через VPN, напрямую сайт был недоступен.

1. Версия —102.6.0esr (64-битная)

Версия браузера —  12.0.1



1. Заходим на сайты, заблокированный роскомнадзором:



Изображение выглядит как текст

Автоматически созданное описание

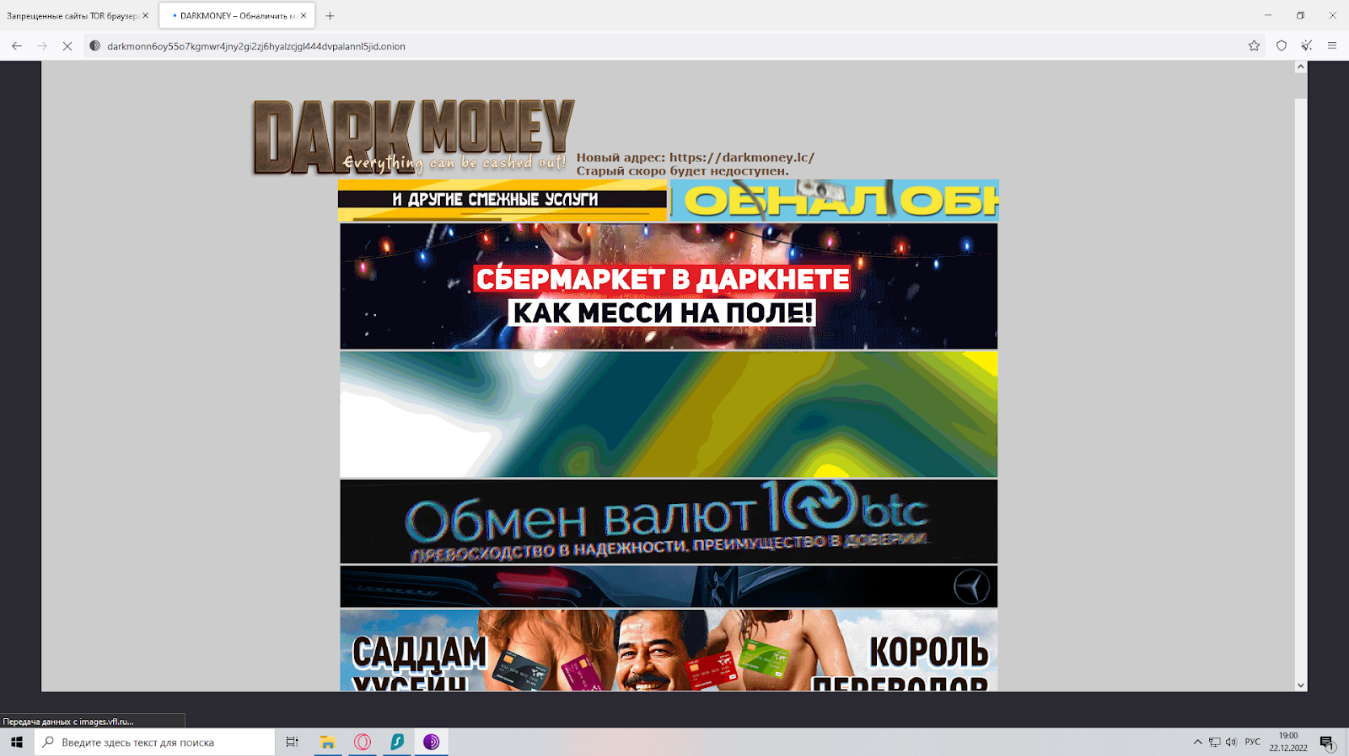
Сайты из списка роскомнадзора открываются спокойно: инстаграм, рутрекер.

Загружаются сайты не быстро, но и не совсем медленно — в общем и целом, терпимо.

Скорее всего, все дело в ВПН, который я использовал.

1. Смотрим сайты с доменом .onion

Решил посмотреть сайт, занимающийся обналом, чтобы не портить психику.



Обычный браузер(Опера) этот сайт, разумеется, не откроет.

Изображение выглядит как текст

Автоматически созданное описание

1. Вывод

**Tor Browser** (сокр. от [англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) ***T****he****O****nion****R****outer*) — [свободное и открытое программное обеспечение](https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%BD%D0%BE%D0%B5_%D0%B8_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) для реализации второго (V2) и третьего (V3) поколения так называемой [луковой маршрутизации](https://ru.wikipedia.org/wiki/%D0%9B%D1%83%D0%BA%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F)[[14]](https://ru.wikipedia.org/wiki/Tor#cite_note-14). Это система [прокси-серверов](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D0%B8-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80), позволяющая устанавливать анонимное [сетевое соединение](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B5_%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5), защищённое от прослушивания. Рассматривается как [анонимная сеть](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%BE%D0%BD%D0%B8%D0%BC%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8) виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. Написана преимущественно на [C](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8_(%D1%8F%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F)).

С помощью *Tor* пользователи могут сохранять [анонимность](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%BE%D0%BD%D0%B8%D0%BC%D0%BD%D0%BE%D1%81%D1%82%D1%8C) в Интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол [TCP](https://ru.wikipedia.org/wiki/TCP). [Анонимизация трафика](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%BE%D0%BD%D0%B8%D0%BC%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%D0%B0) обеспечивается за счёт использования распределённой сети серверов — [узлов](https://ru.wikipedia.org/wiki/%D0%A3%D0%B7%D0%B5%D0%BB_%D1%81%D0%B5%D1%82%D0%B8)[[17]](https://ru.wikipedia.org/wiki/Tor#cite_note-17). Технология *Tor* также обеспечивает защиту от механизмов анализа трафика[[18]](https://ru.wikipedia.org/wiki/Tor#cite_note-18), которые ставят под угрозу не только [приватность в Интернете](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%B2%D0%B0%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5), но также конфиденциальность [коммерческих тайн](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BC%D0%B5%D1%80%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%82%D0%B0%D0%B9%D0%BD%D0%B0), деловых контактов и [тайну связи](https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D0%B9%D0%BD%D0%B0_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8) в целом.

Tor можно использовать в качестве прокси-сервера для обхода блокировок. Из-за “безопасности” пользователя в этом браузере появляется возможность для организации сайтов и сервисов сомнительного, мягко говоря, характера. Либо попытаться попробовать контент, запрещенный в России.

Браузер я, конечно, удалю, тёмная сторона интернета меня не интересует.