

Федеральное государственное бюджетное образовательное учреждение  
Высшего профессионального образования  
Южно-уральский Государственный Университет  
(Национальный исследовательский университет)

Исследовательская работа  
на тему:  
«Противодействие кибертерроризму,  
совершаемому в deepweb»

**Выполнила:**

Студентка гр. КТУР-168

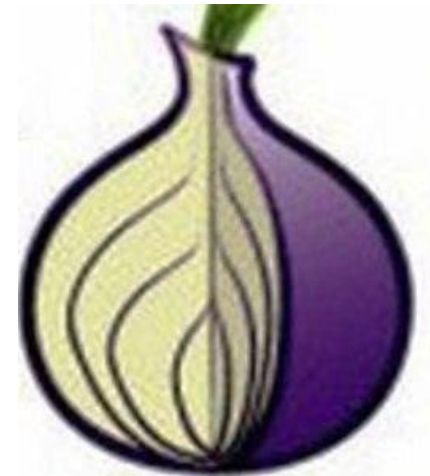
Каримова А.В.

Челябинск, 2015

**Цель работы:** Поиск путей защиты населения от распространения незаконных интернет - материалов и запрещенных товаров, совершаемого путем анонимного доступа с помощью маршрутизации «Onion routing» и противодействие кибертерроризму, совершаемому в deepweb.

**Задачи:**

- изучить понятийный аппарат и актуальность проблемы,
- исследовать структуру уровней анонимности интернет-страниц,
- проанализировать принцип работы анонимных сервисов, работающих на основе «луковой маршрутизации»,
- предложить как один из вариантов решения проблемы систему полной блокировки серверов для самых популярных сервисов, работающих на принципе маршрутизации «Onion routing», в частности, Tor.



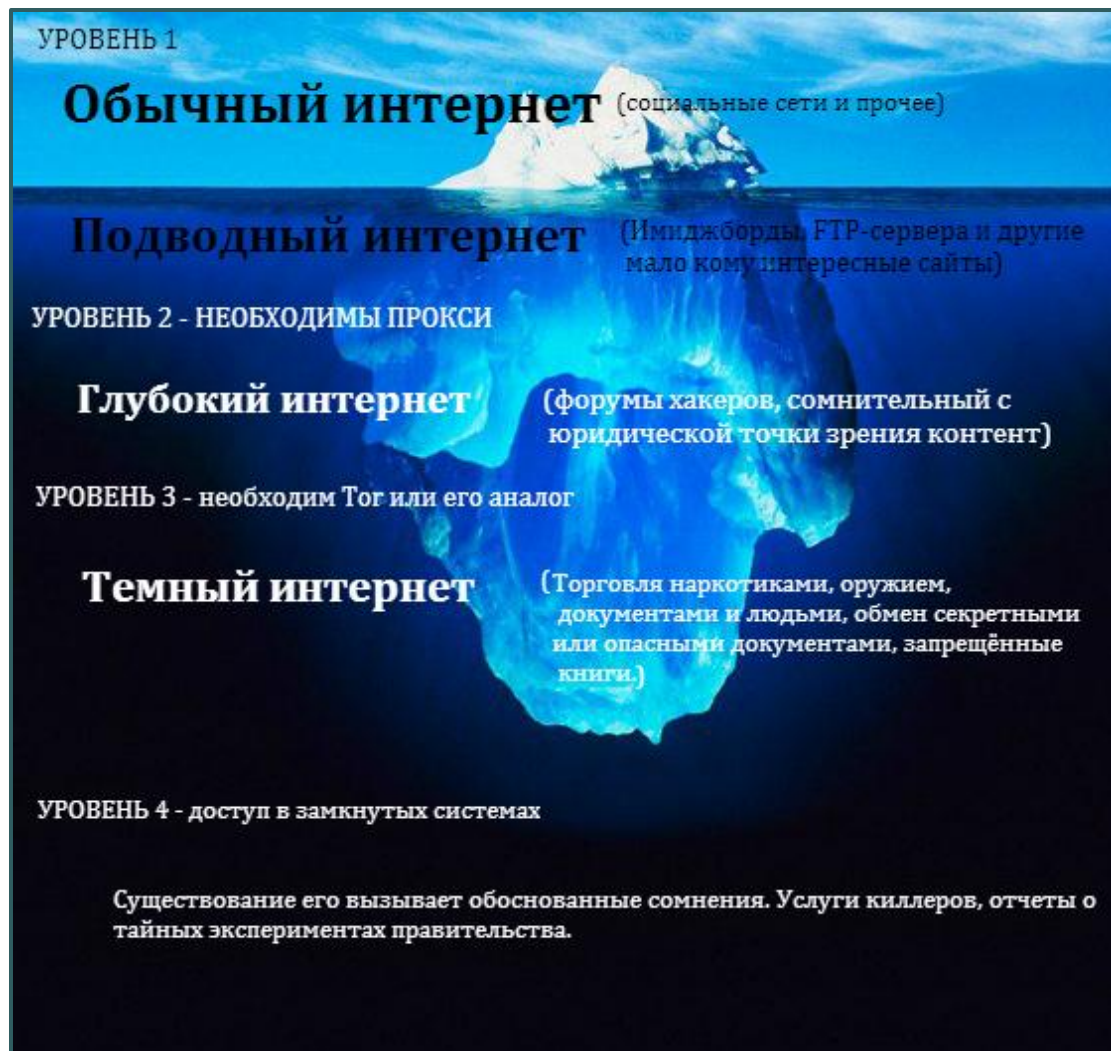
# Основные понятия

- Deepweb - сегмент сети Интернет, не поисковыми системами.
- Кибертерроризм- совершение незаконных действий в сети.
- Анонимность – способ доступа в сеть, сохраняющий данные и их отправителя и получателя в конфиденциальности.

## Крупные русскоязычные сайты deepweb'a

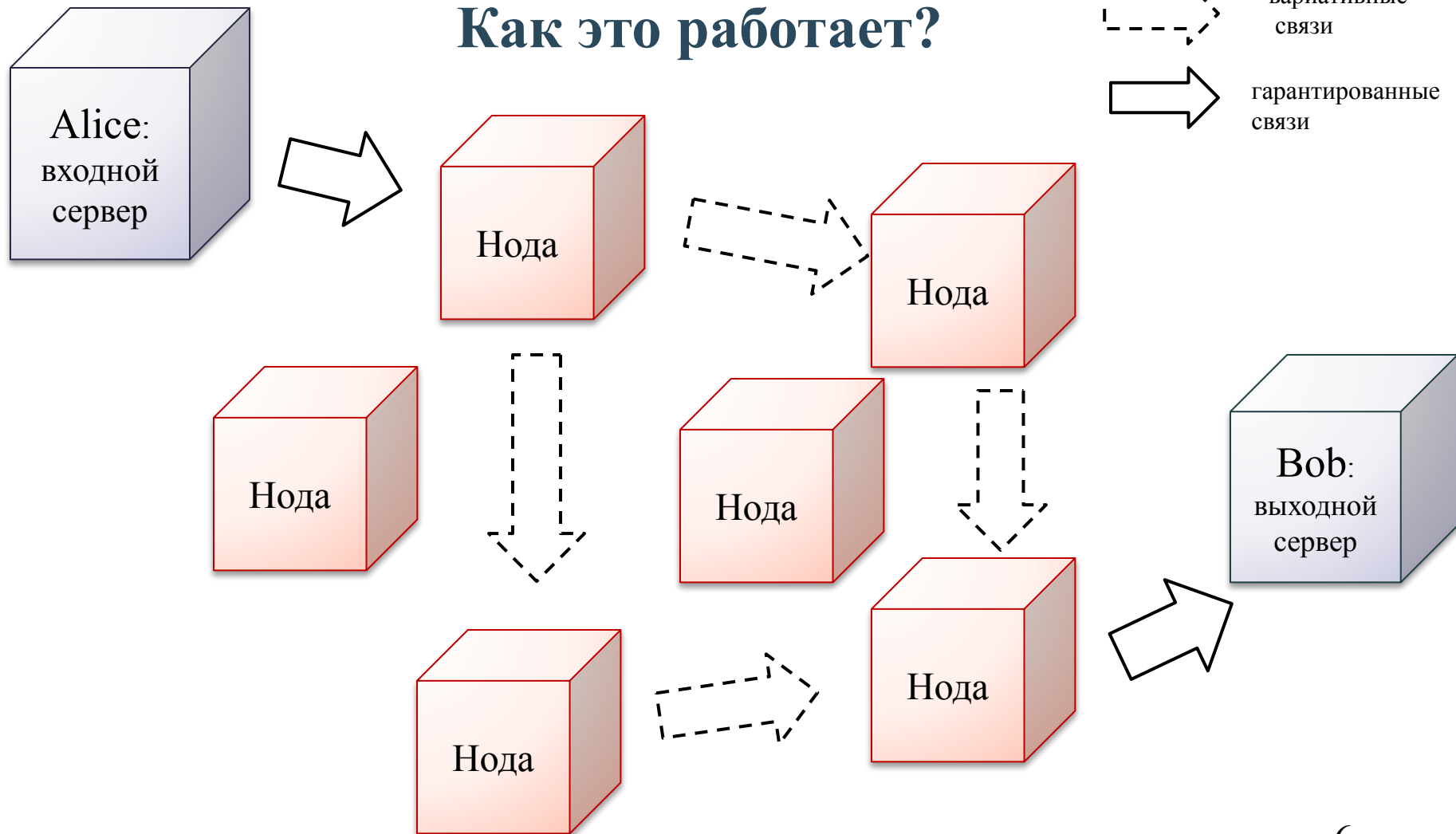
- **Runion.** Крупный русскоязычный форум с разделами на тему около-незаконных вещей. Обсуждают все - от нанесения физического вреда и покупки оружия до статей на тему социальной инженерии, от советов, как вести тебя на допросе, до способов атаки на программное обеспечение в самых разных сферах.
- **RAMP.** Крупнейший русскоязычный магазин запрещенных веществ. Приобрести можно все, что угодно, кроме редких наркотиков и героина, на такой товар у большинства местных продавцов табу.

# Уровни анонимности интернета



Для доступа к Deepweb (уровень 3 и ниже) используются анонимные сервисы наподобие Tor.

# Как это работает?



## Как это работает?

случайным образом выбирается цепочка серверов, через которую будет идти весь трафик

входной сервер (Alice) зашифровывает данные столько раз, сколько серверов-нод(+) в цепочке

промежуточные сервера снимают шифрование "послойно", как кожуру с лука

выходные данные в чистом виде можно отследить только с помощью анализа выходного(Bob) сервера

**Проблема:** распространение незаконных интернет - материалов и запрещенных товаров, совершаемых путем анонимного доступа с помощью маршрутизации «Onion routing» и противодействие кибертерроризму, совершаемому в deepweb.

**Вариант решения:** полная блокировка всех серверов Тора у всех провайдеров.



Написать скрипт, который будет многократно проверять все существующие адреса серверов Тора, находящиеся по адресу <https://globe.torproject.org> и при обнаружении незаблокированного сервера добавлять его в «черный» список.



# Мнение общественности

- **Только так мы сможем значительно минимизировать объемы незаконных продаж наркотиков, нелегального оружия и другой противозаконной деятельности и защитить молодое поколение от пагубного влияния Deepweb.**
- Разблокируйте мой сервер!
- Почему нас ограничивают в доступе?
- Я хочу работать в анонимной сети!

## Библиографический список

1. [torproject.org](http://torproject.org) – официальный сайт Tor.
2. [habrahabr.ru/post/194046/](http://habrahabr.ru/post/194046/) - информация о уязвимостях сервиса.
3. [ru.wikipedia.org/wiki/Tor](http://ru.wikipedia.org/wiki/Tor) - принцип работы Тора.