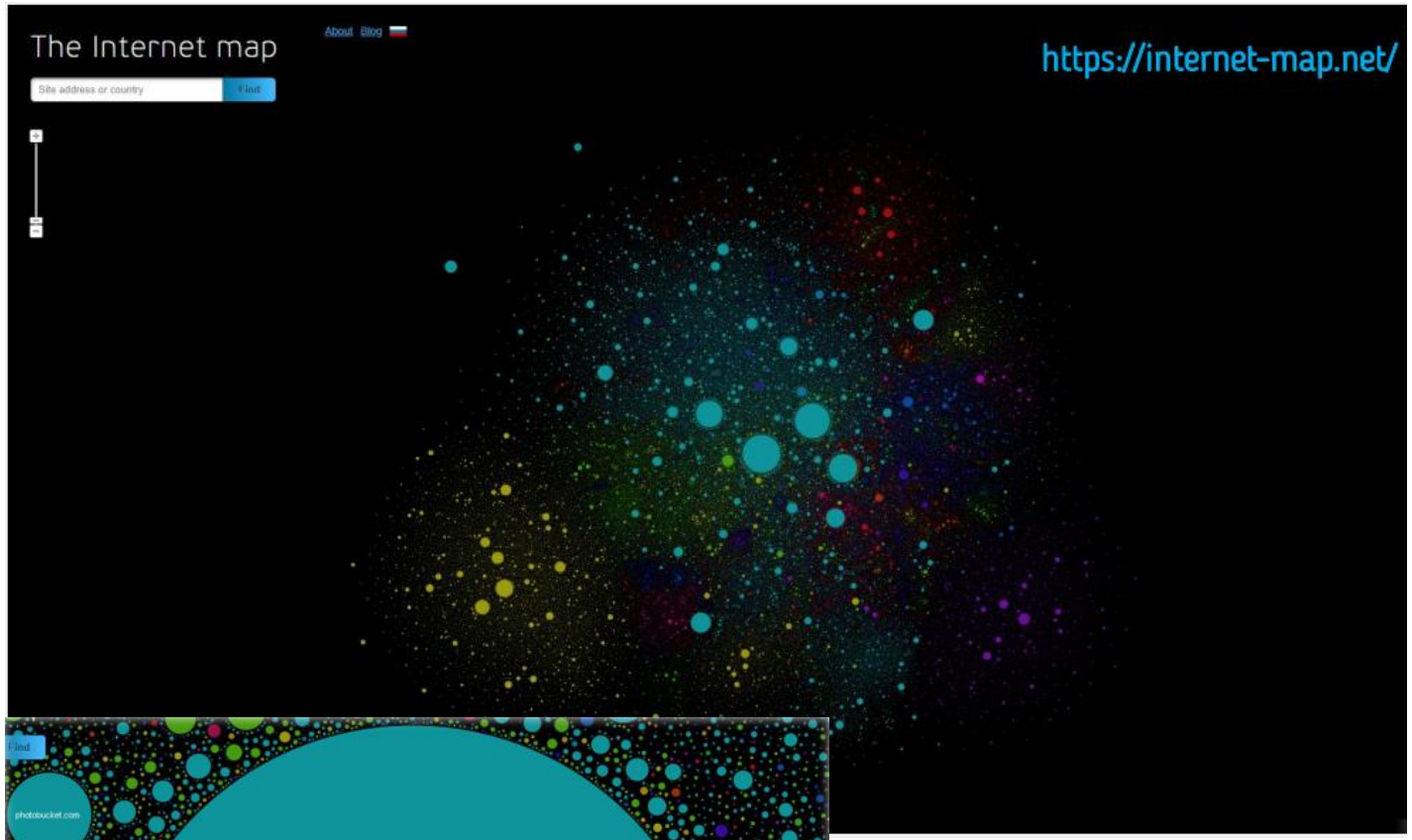
# Цифровизация образования и информационная безопасность в интернете

Змеев Михаил Владимирович

# BigData: новые правила жизни в сети

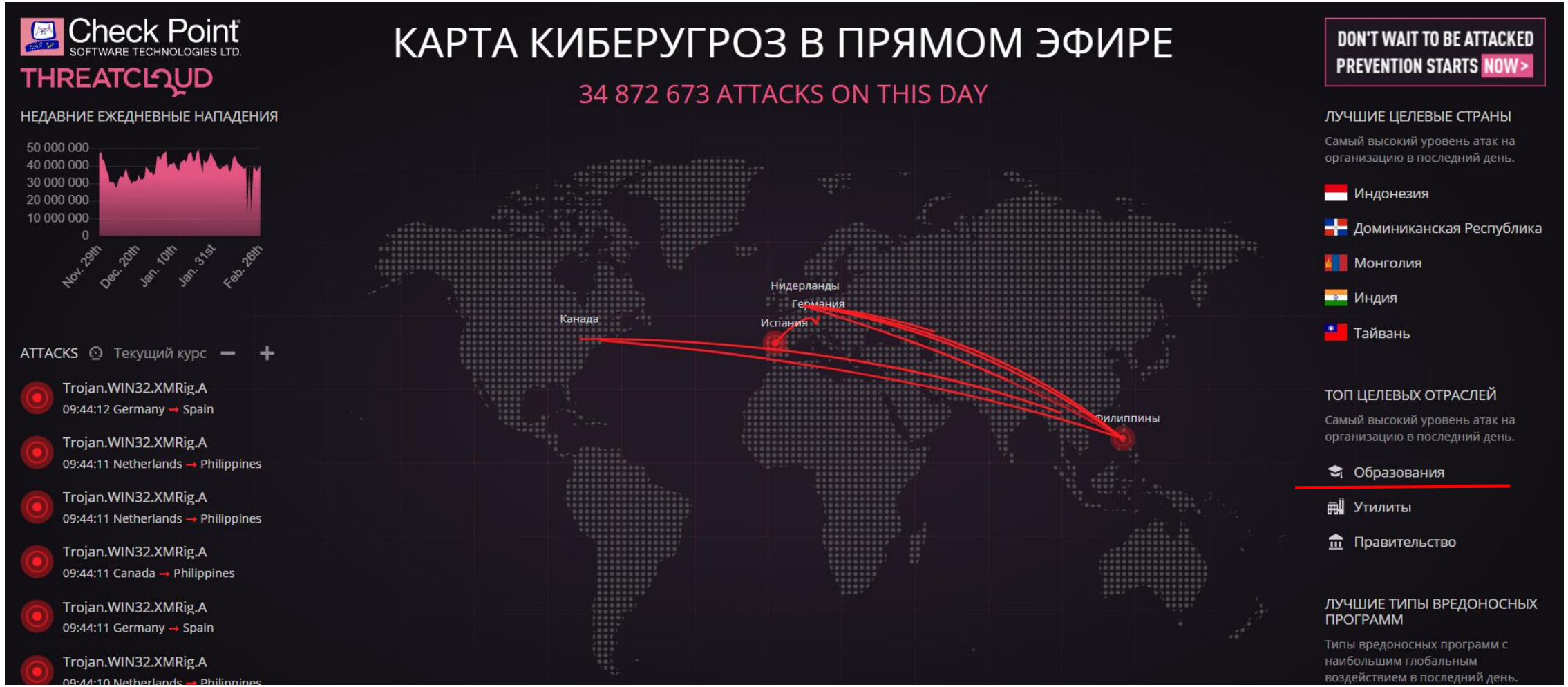
- Цифровизация – неотъемлемая часть нашей реальности
- У цифровой «вселенной» есть свои правила функционирования, свои ловушки и опасности
- «Не знаешь броду – не  суйся в воду»



Рядом с большими ресурсами – ресурсы спутники

# https://cybermap.kaspersky.com/ru/

# https://threatmap.checkpoint.com/



# Ключевые аспекты цифровой безопасности

- Защита персональных данных
- Защита гаджетов и ПК от вирусов
- Использование лицензионного контента и ПО
- Грамотное хранение информации (особенно персональной)
- Цифровой этикет и репутация в интернете

# Цифровая безопасность: на чем покоится?

- **Конфиденциальность**

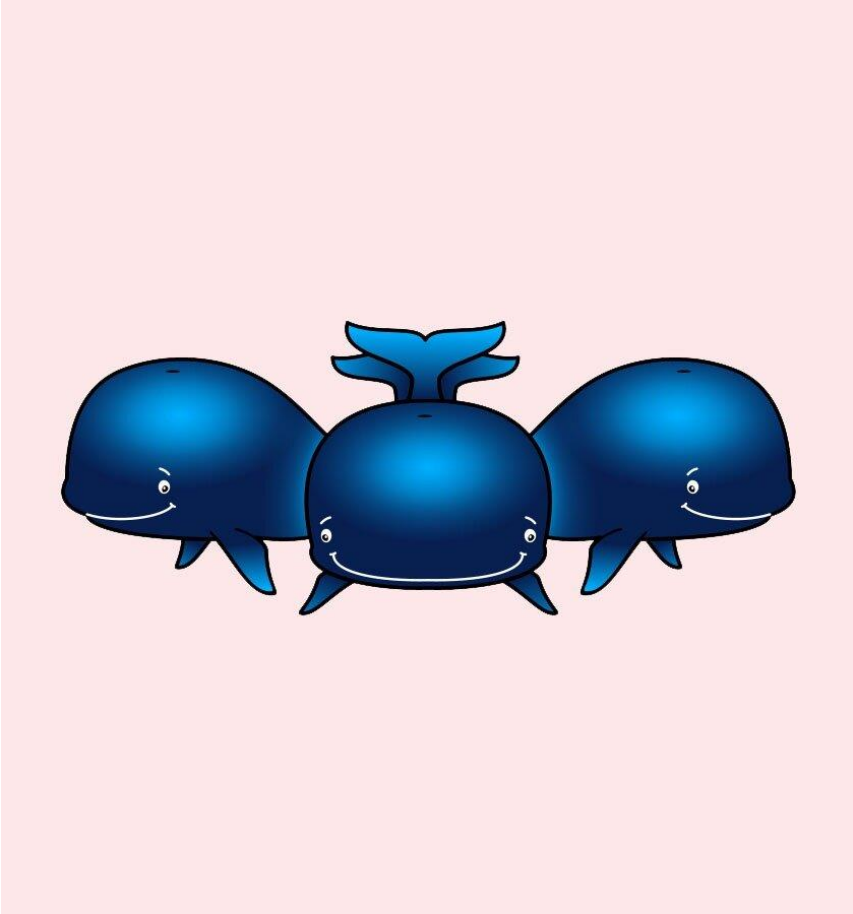
(неразглашение и утечка информации: *утеря пароля*)

- **Целостность**

(сохранность данных при операциях: *потеря при передаче*)

- **Доступность**

(беспрепятственный доступ к информации: *отказ сайта*)



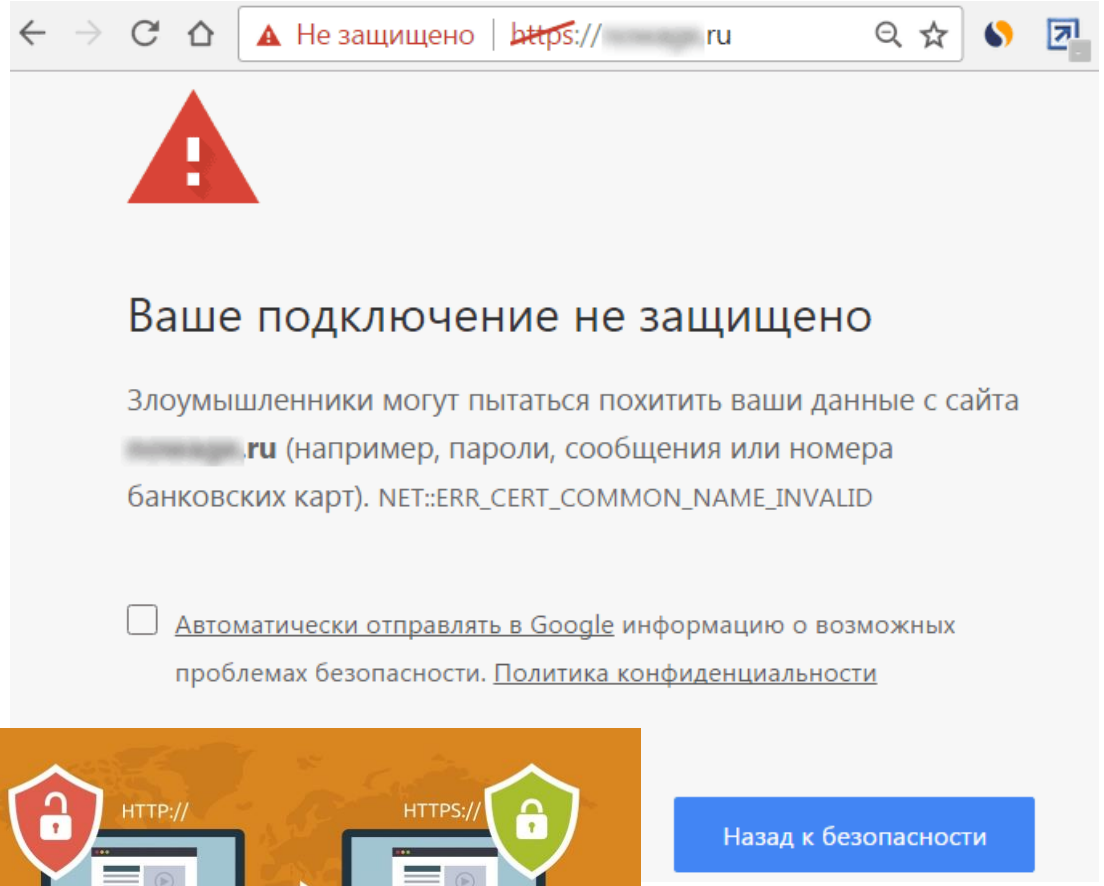
# Безопасность: общие правила

- Неуязвимых систем не существует!
- Пользуйтесь проверенными и защищенными ресурсами!
- Странное (необычное) поведение системы в интернете – повод насторожиться!
- То, что попало в сеть – не удаляется!
- Следовательно, если нет необходимости что-то конфиденциальное выкладывать в сеть, – не выкладывать!

# Конфиденциальность (защита данных)

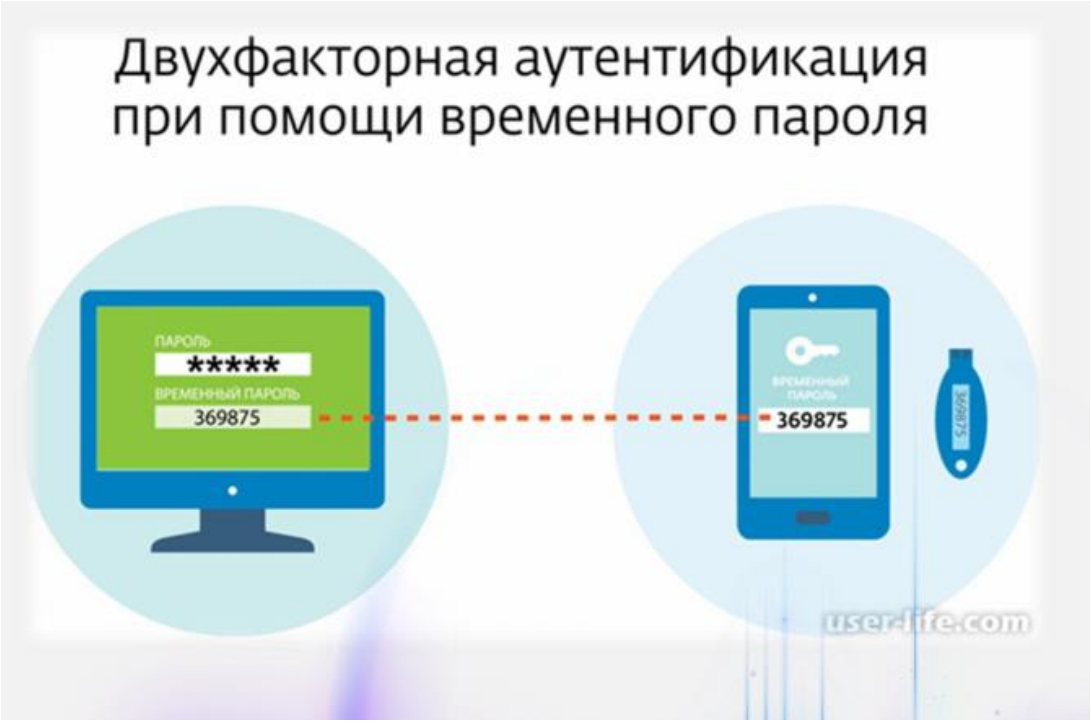
**Правило 1**

- Защищенное соединение используется, чтобы особо важные данные передавать скрытно от посторонних.
- Они сначала подвергаются изменению (шифруются), затем отправляются на сервер.
- **Таким образом, «подслушать» что-либо злоумышленнику не удастся.**



**Правило 2**

- Для защиты важной персональной информации (*почта, банкинг и т.д.*) желательно пользоваться двухфакторной аутентификации




**Правило 3**

- Не доверяйте/проверяйте общедоступные Wi-Fi сети (*можно получить доступ к банковским учетным данным, паролям к учетным записям)*

**Правило 3**

- Децентрализация хранения информации на разных почтовых ящиках

**Правило 4**

- Не создавайте один пароль для разных сайтов/сервисов/блогов

# Культура цифрового образования

- Используйте проверенные и безопасные площадки образования
- При проектировании задания с использованием сетевых ресурсов, проверьте сами ресурсы
- Формируйте у учеников «копилку» качественного контента

ПостНаука
postnauka.ru

Открытое образование

Лекториум

Arzamas

GOU
Gaidar Open University

coursera

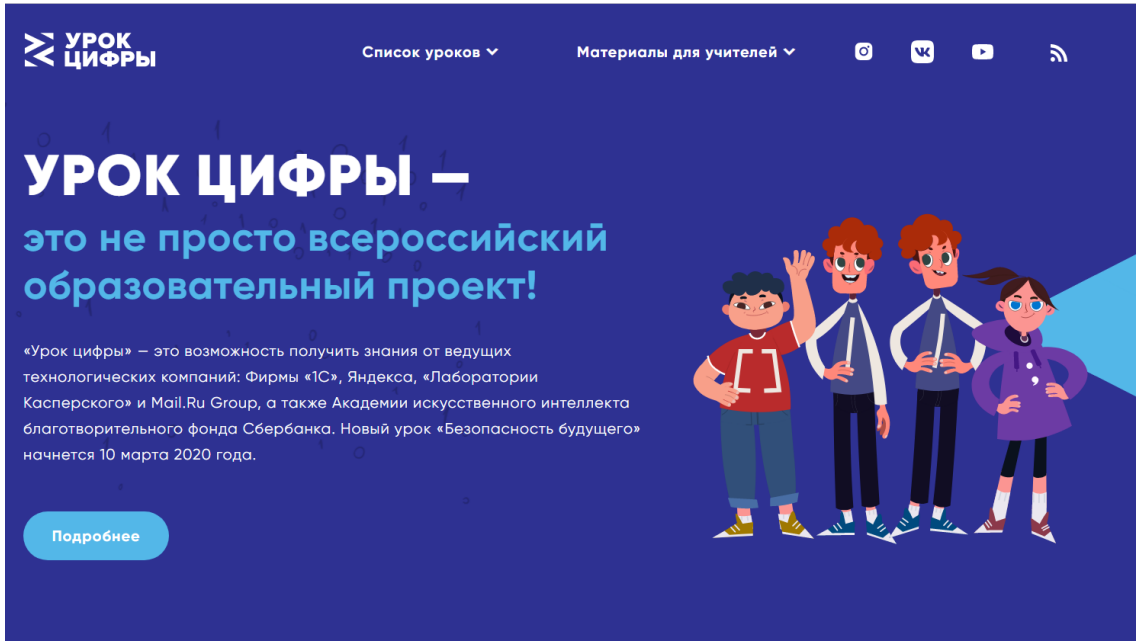
ИСТОРИЯ.РФ
исторический портал

СДАМ ГИА: РЕШУ ЕГЭ
Образовательный портал для подготовки к экзаменам
Математика профильного уровня

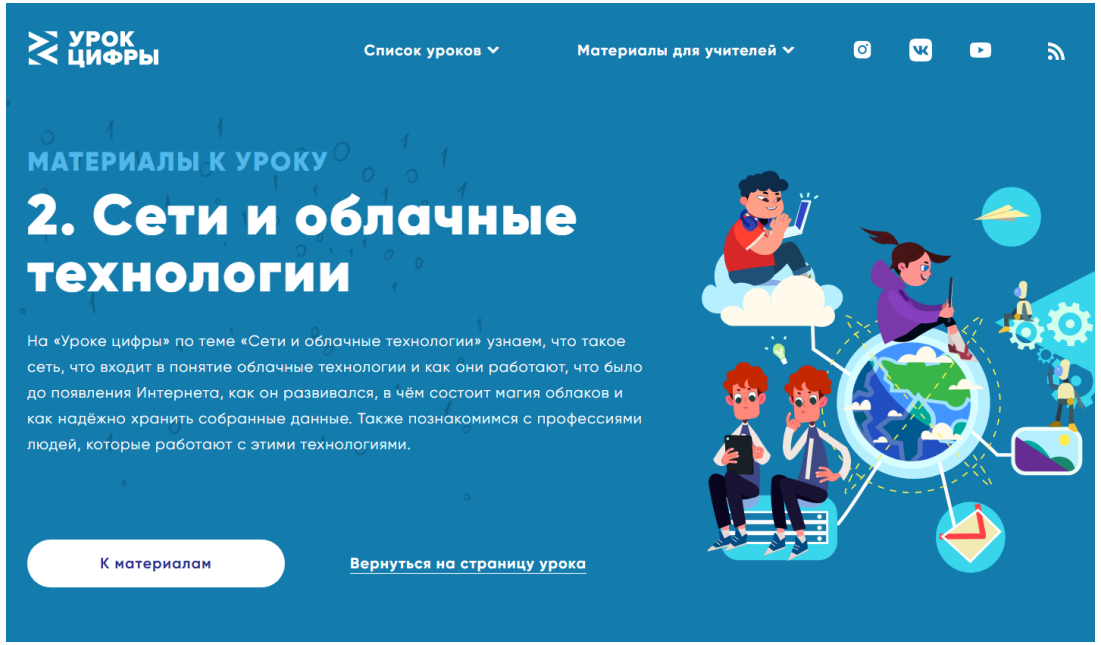
# Эффективные каналы коммуникации с учениками в сети

1. Электронная почта
2. Сайт педагога
3. Каналы в мессенджерах (!)
4. Социальные сети (закрытые группы)

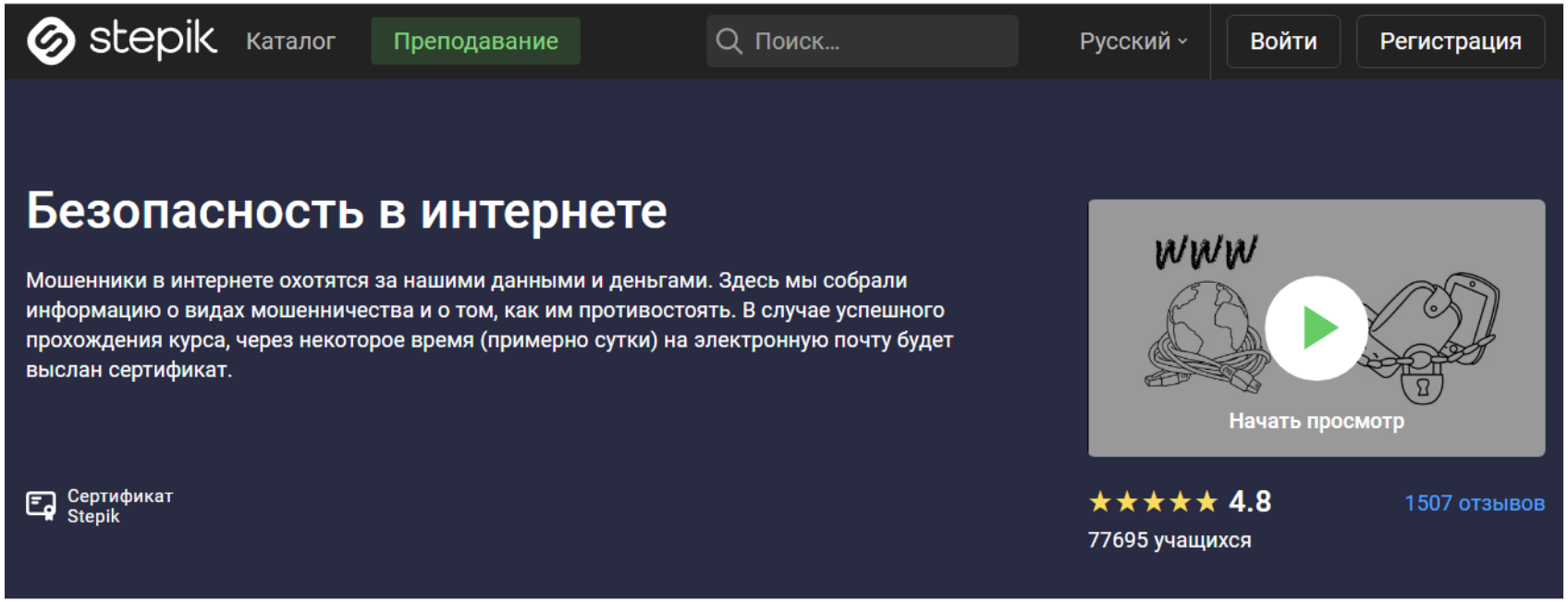
# Учить цифровой безопасности




https://xn--h1adlhdnlo2c.xn--p1ai/



https://stepik.org/course/191/promo




Академия Яндекса

Бесплатно

Поступить на курс

О курсе

# Блогинг Лаборатории Касперского

- https://www.kaspersky.ru/blog/category/threats/

Спасибо за внимание!

Универсум

АНО Центр НИОКР

+7 (912) 014-31-13
director@ano-universum.ru
https://ano-universum.ru/