

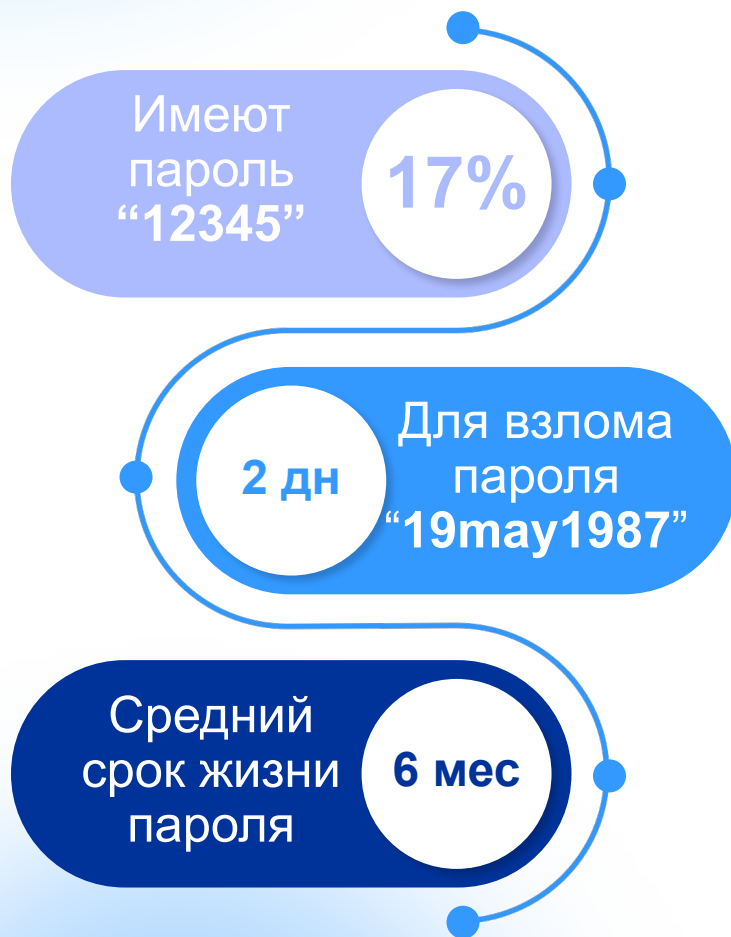


**ИТ-класс**  
В МОСКОВСКОЙ ШКОЛЕ

# Цифровая безопасность

**Дьяконов Егор Николаевич**

# Парольная безопасность



## Что-то большее, чем пароль

- 1 SMS и push сообщения
- 2 Устройства: донглы и карточки доступа
- 3 Биометрия: отпечаток пальца или распознавание лица
- 4 Смартфон: требование выполнить определенные действия



# Публичный **WiFi**



**WiFi**

**подмена**



Считывание трафика с вашей устройства



Создание поддельных веб сайтов и перенаправление



Работа в сети от имени вашего устройства



## Рекомендации экспертов

1

### Правило минимума

Предоставляйте сервисам минимальный набор данных необходимый для получения услуги, приобретения товара

2

### Соблюдайте цифровую гигиену

не размещайте много данных о себе в соцсетях – их могут использовать против вас



## Рекомендации экспертов

3

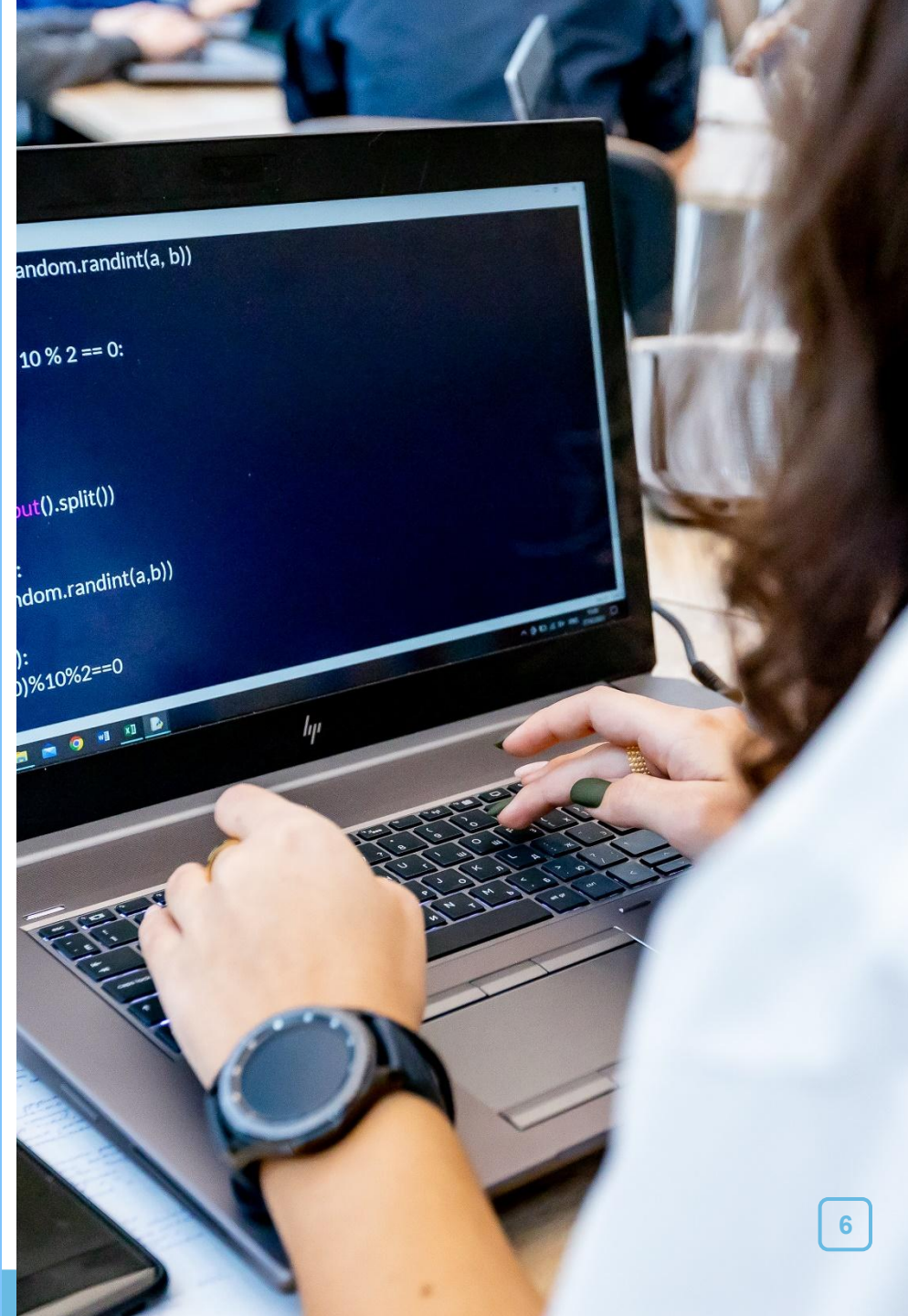
### Режим паранойи

Не переходите по сомнительным ссылкам в e-mail и мессенджерах, не вводите на подозрительных ресурсах учетные данные и другие важные сведения

4

### Не разрешаю!

Не устанавливайте ПО на устройства с сайтов, изучайте отзывы на разработчика. Если приложение требует разрешения, которые не соотносятся с его целями, оно **будет** скрывать вредоносные функции



## Рекомендации экспертов

5

### Не торопитесь!

У вас всегда должно быть время для принятия решения. Если вас лишают этого времени, не дают убедиться в достоверности информации, то вы имеете дело с мошенником.

6

### Молчите!

Не разглашайте коды подтверждения, особенно, если в тексте смс-сообщения или пуш-уведомления.



# Проверим ваше устройство на безопасность!

Перейдите по QR-коду для:



Сканирования устройства на встроенные уязвимости



Проверки поступивших сообщений на спам и фишинг



Проверки сохраненных паролей на устройстве \*



\* на предмет встречи хэша пароля в базе данных известных пар хэш-пароль от *Yandex.Research Security*.

# Нейросети творят

- ▶ **Deep learning** (глубинное обучение) генеративно-сопоставительной сети (Generative Adversarial Network, или GAN).
- ▶ Машине «скармливают» неструктурированные данные в виде изображения лица того или иного человека, после этого происходит построение двухмерного образа с втягиванием его в трехмерную перспективу видеоролика.



*Пока данная технология не совершенна, можно распознать подделку по некоторым деталям. Нос. Почему-то его направление, как правило, не совпадает с физиологически обусловленным. Неровное движение, отсутствие моргания глаз, разные оттенки кожи, плохая синхронизация губ с речью.*