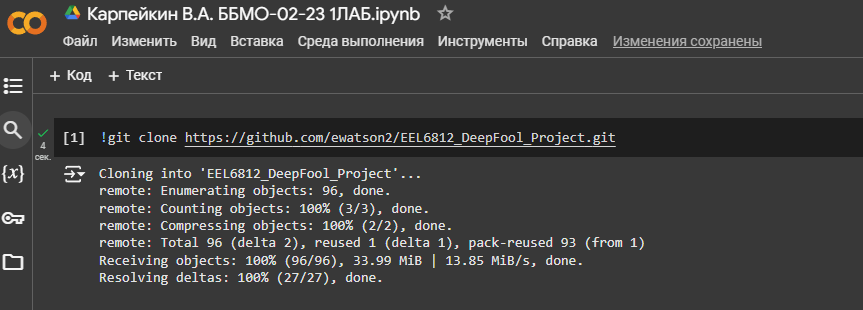
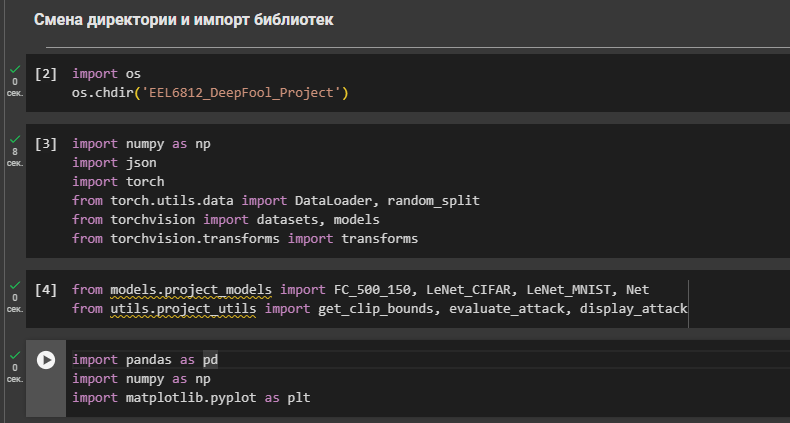
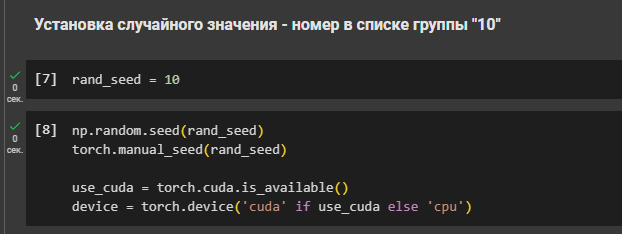
**Карпейкин В.А. ББМО-02-23 Номер 10**

**Клонирование репозитория**

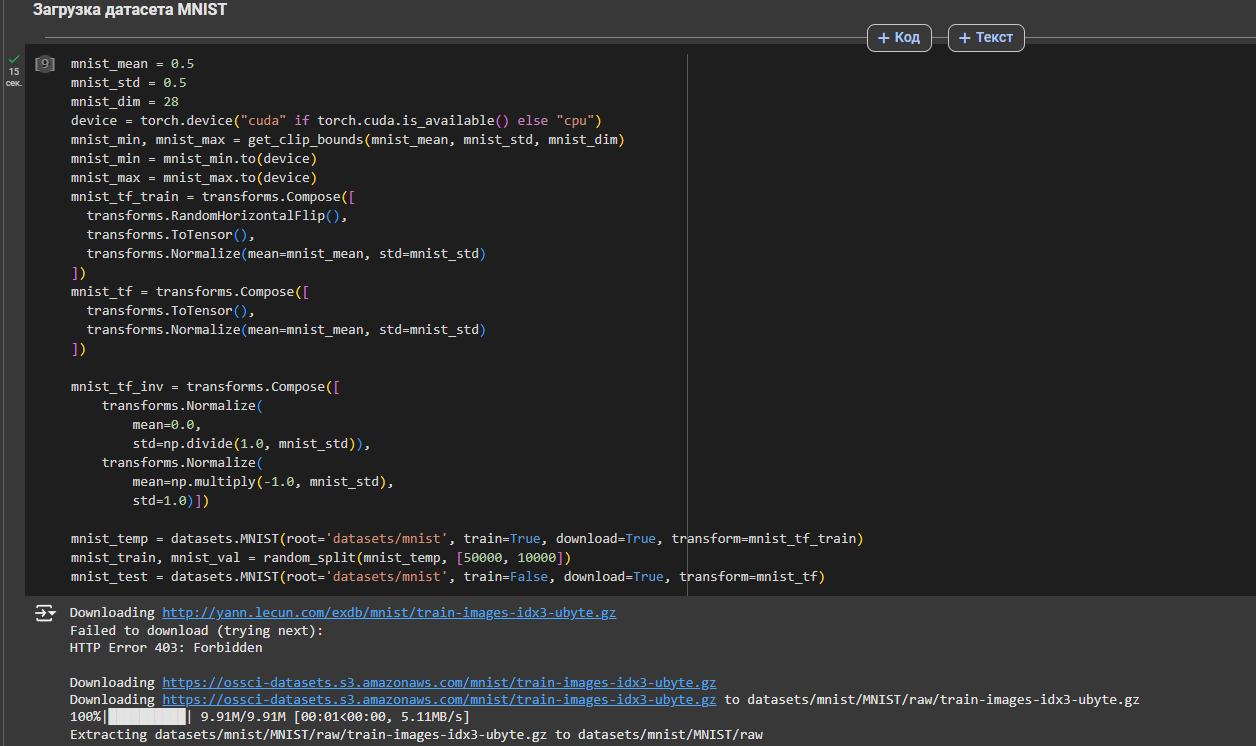


**Смена директории и импорт библиотек**

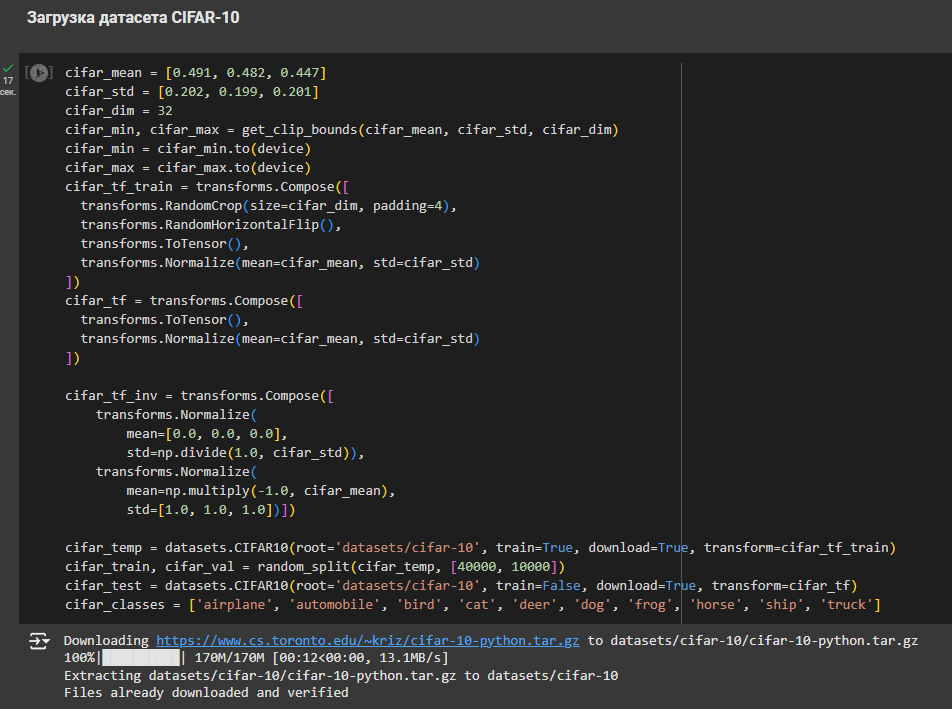


**Установка случайного значения – номер в списке группы «10»** 

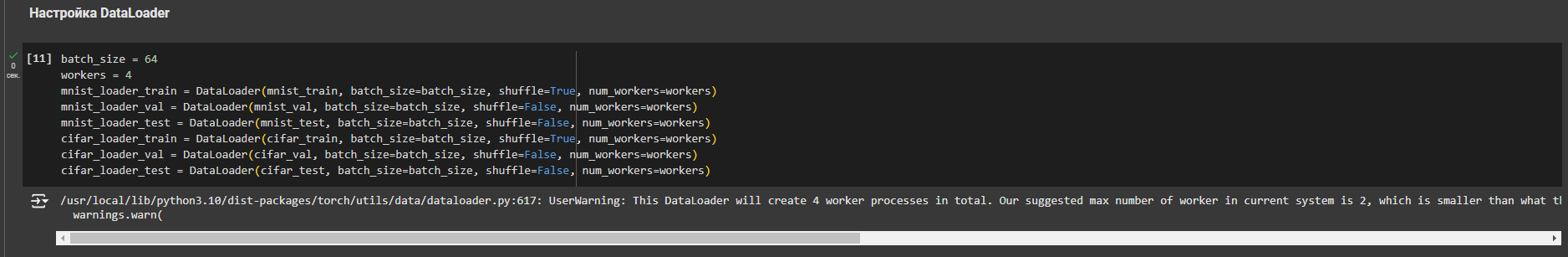
**Загрузка датасета MNIST**



**Загрузка датасета CIFAR-10**



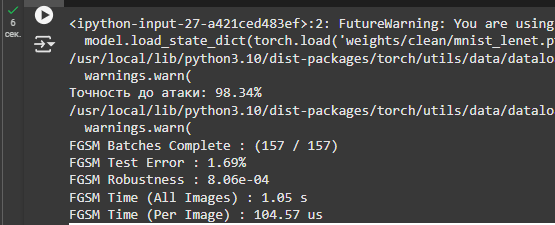
**Настройка DataLoader**



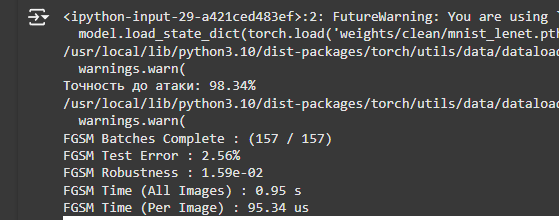
**FGSM атака**

**Стойкость к атаке моделей LeNet, FC на датасете MNIST и стойкость к атаке моделей Network-In-Network, LeNet на датасете CIFAR-10**

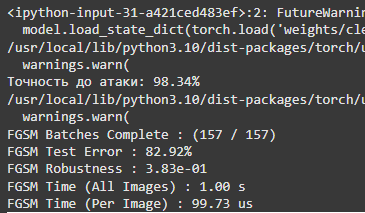
**LeNet MNIST**

fgsm\_eps = 0.001 

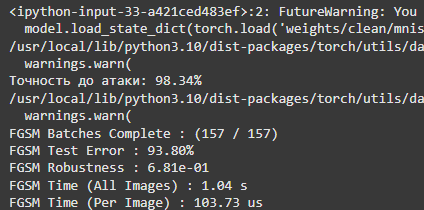
fgsm\_eps = 0.02



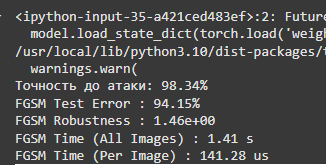
fgsm\_eps = 0.5



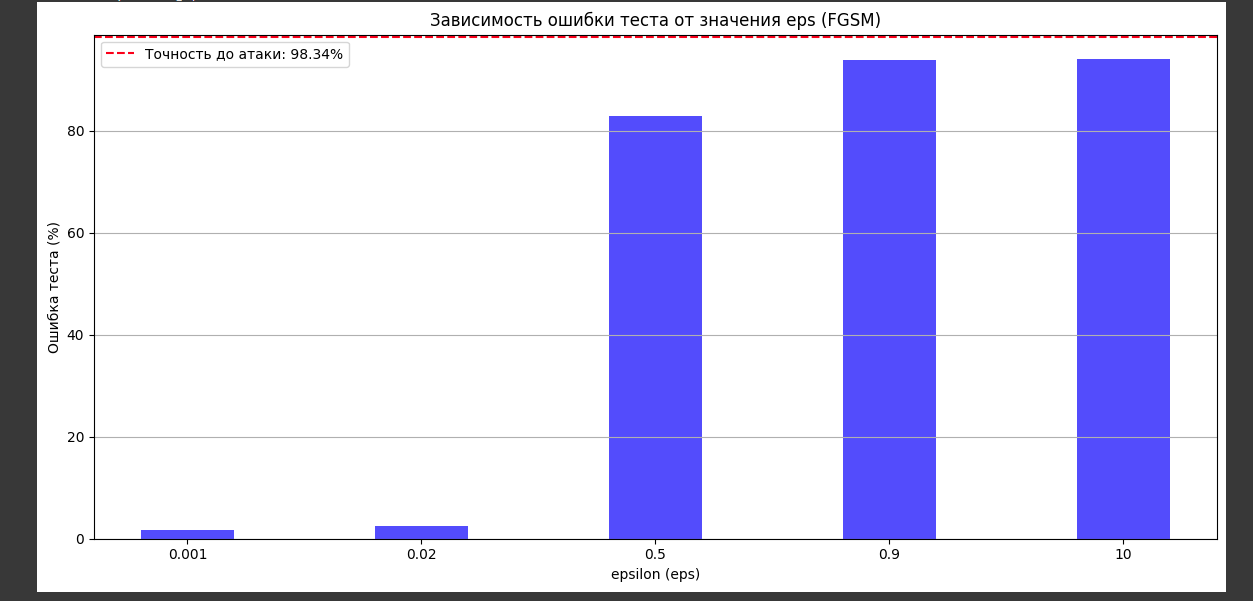
fgsm\_eps = 0.9



fgsm\_eps = 10

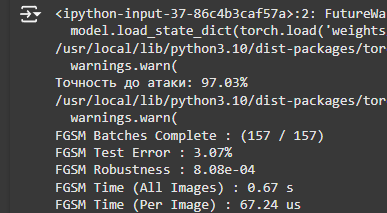


**График**

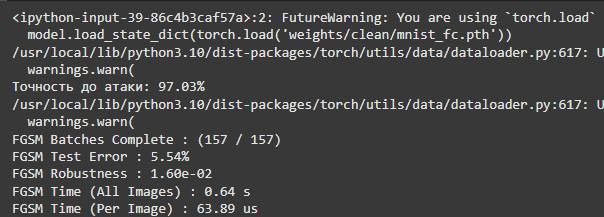


**FC MNIST**

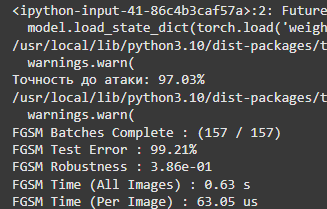
fgsm\_eps = 0.001



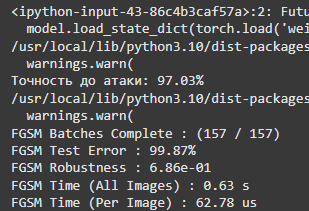
fgsm\_eps = 0.02



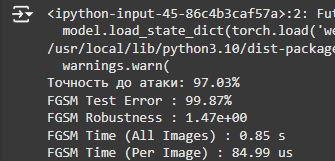
fgsm\_eps = 0.5

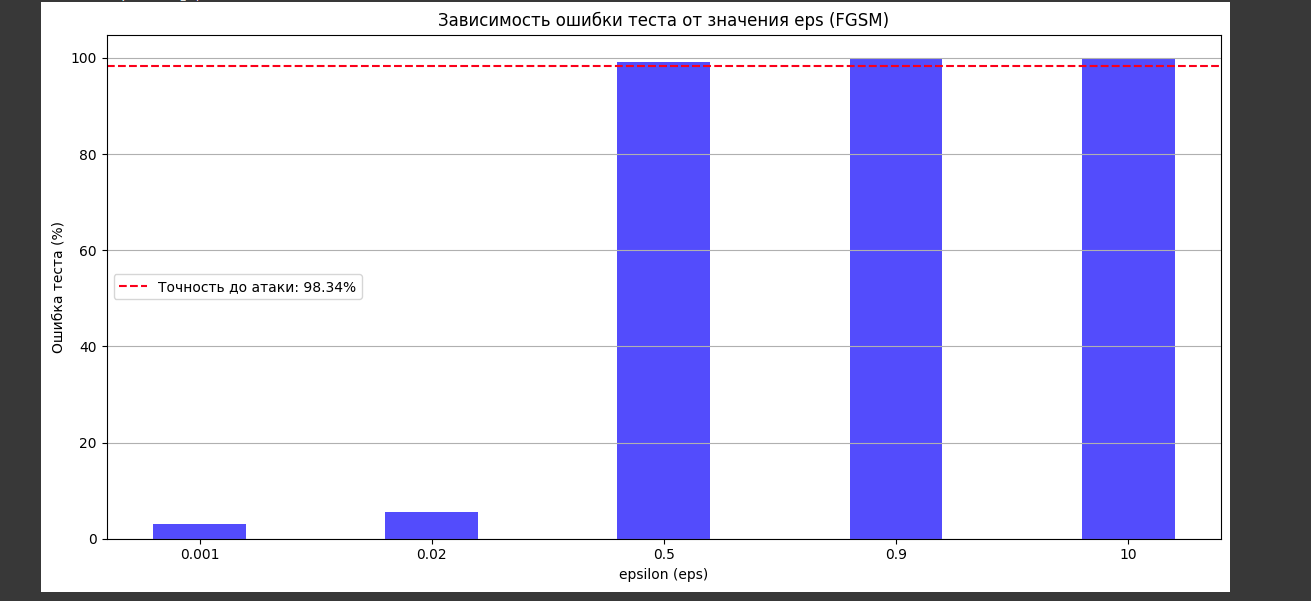


fgsm\_eps = 0.9

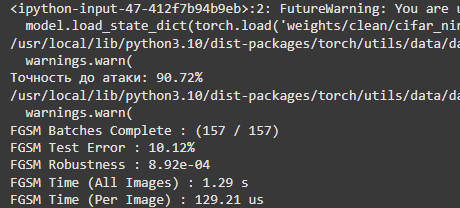


fgsm\_eps = 10

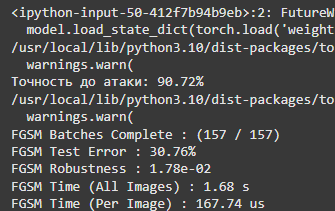


**График** 

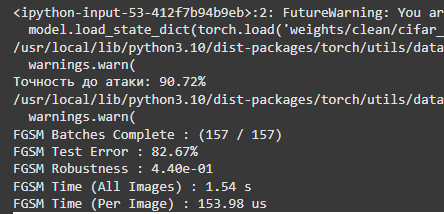
**Network-In-Network CIFAR-10**

fgsm\_eps = 0.001 

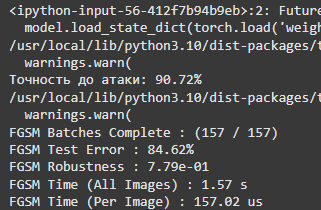
fgsm\_eps = 0.02



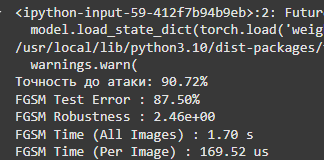
fgsm\_eps = 0.5

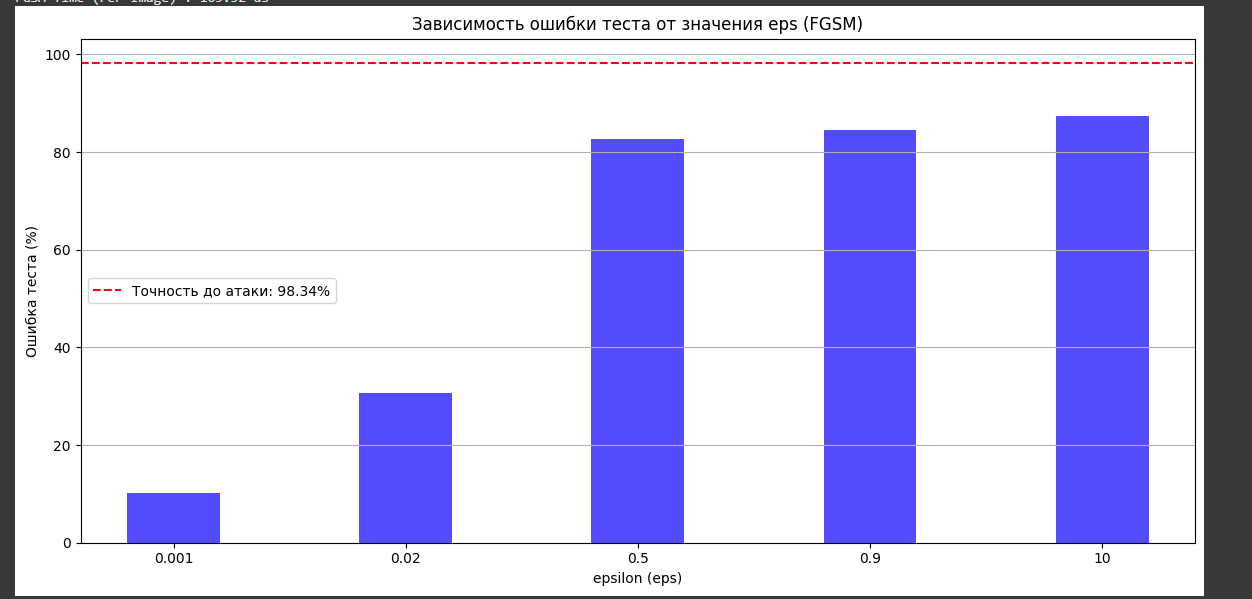


fgsm\_eps = 0.9



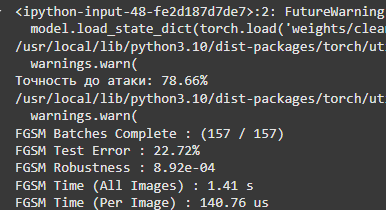
fgsm\_eps = 10



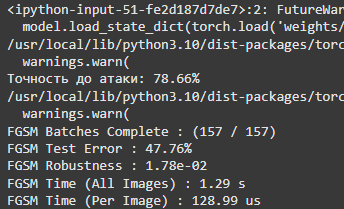
**График** 

**LeNet CIFAR-10**

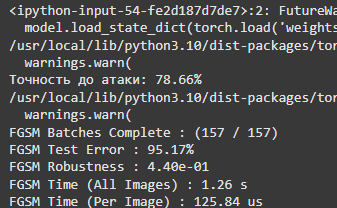
fgsm\_eps = 0.001



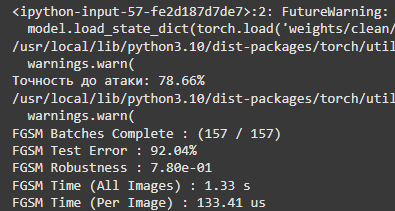
fgsm\_eps = 0.02



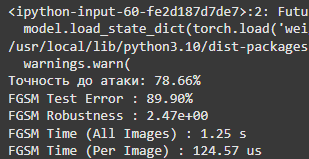
fgsm\_eps = 0.5

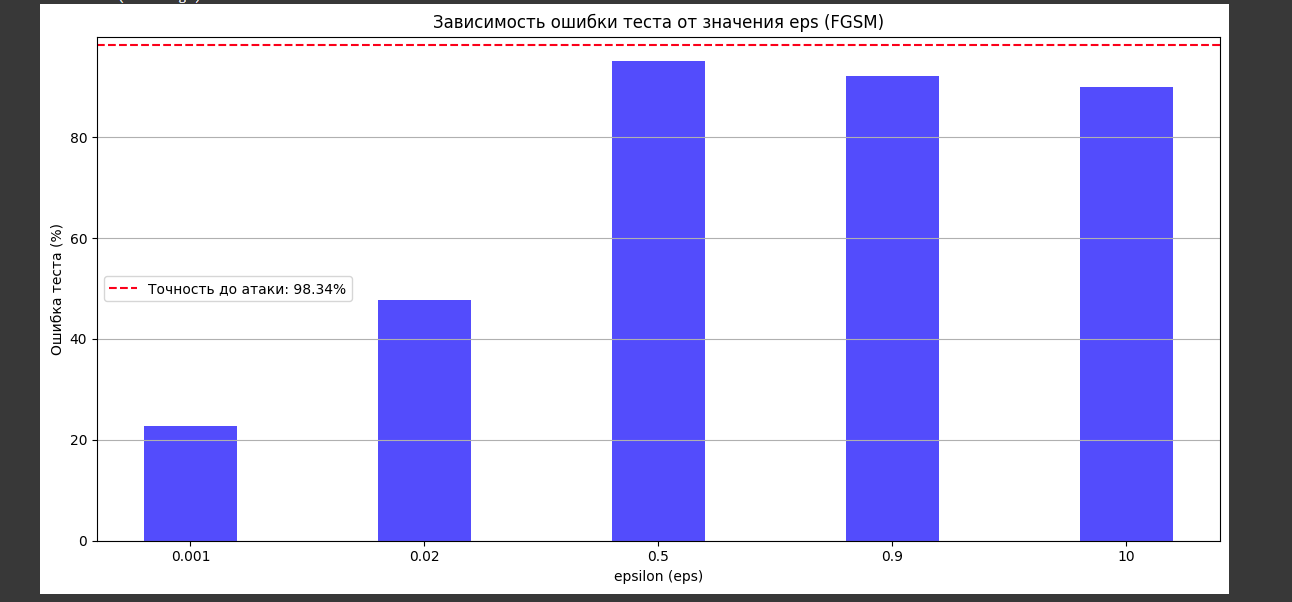


fgsm\_eps = 0.9



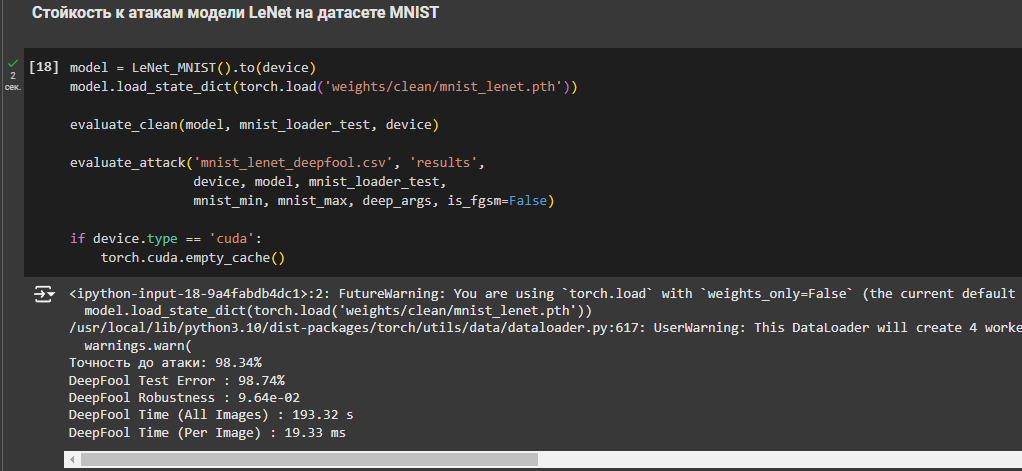
fgsm\_eps = 10

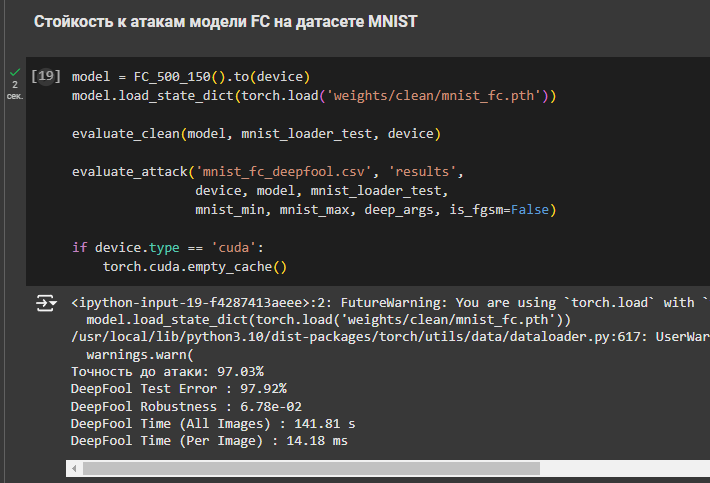


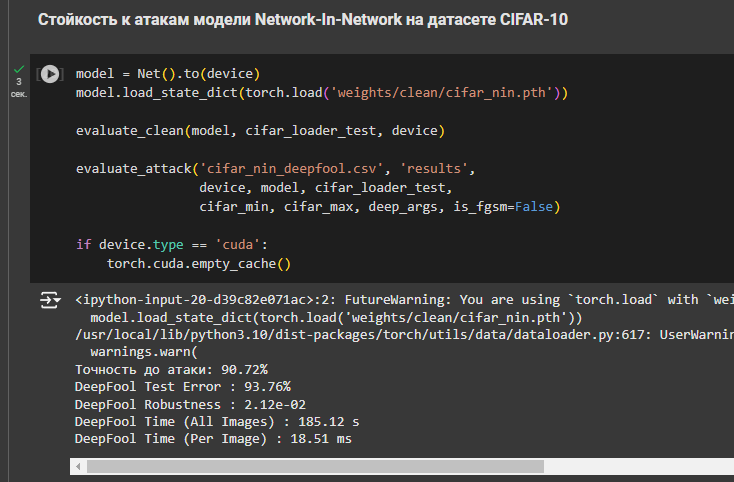
**График** 

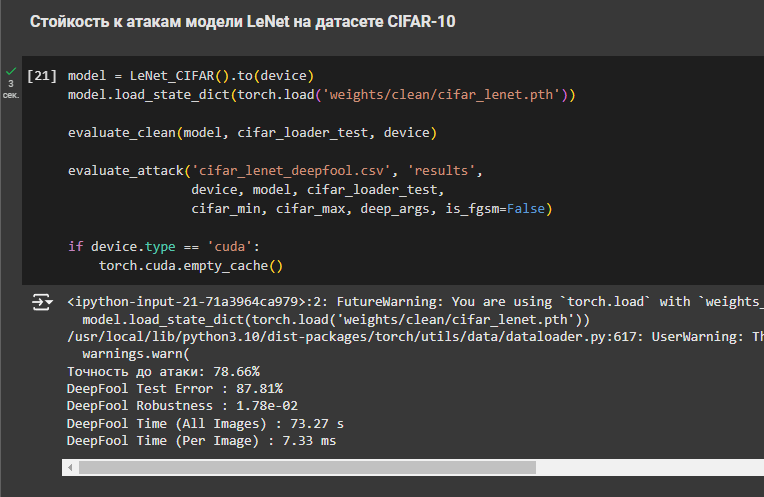
**DeepFool атака**

**Стойкость к атаке моделей LeNet, FC на датасете MNIST и стойкость к атакае моделей Network-In-Network, LeNet на датасете CIFAR-10**

**LeNet MNIST** 

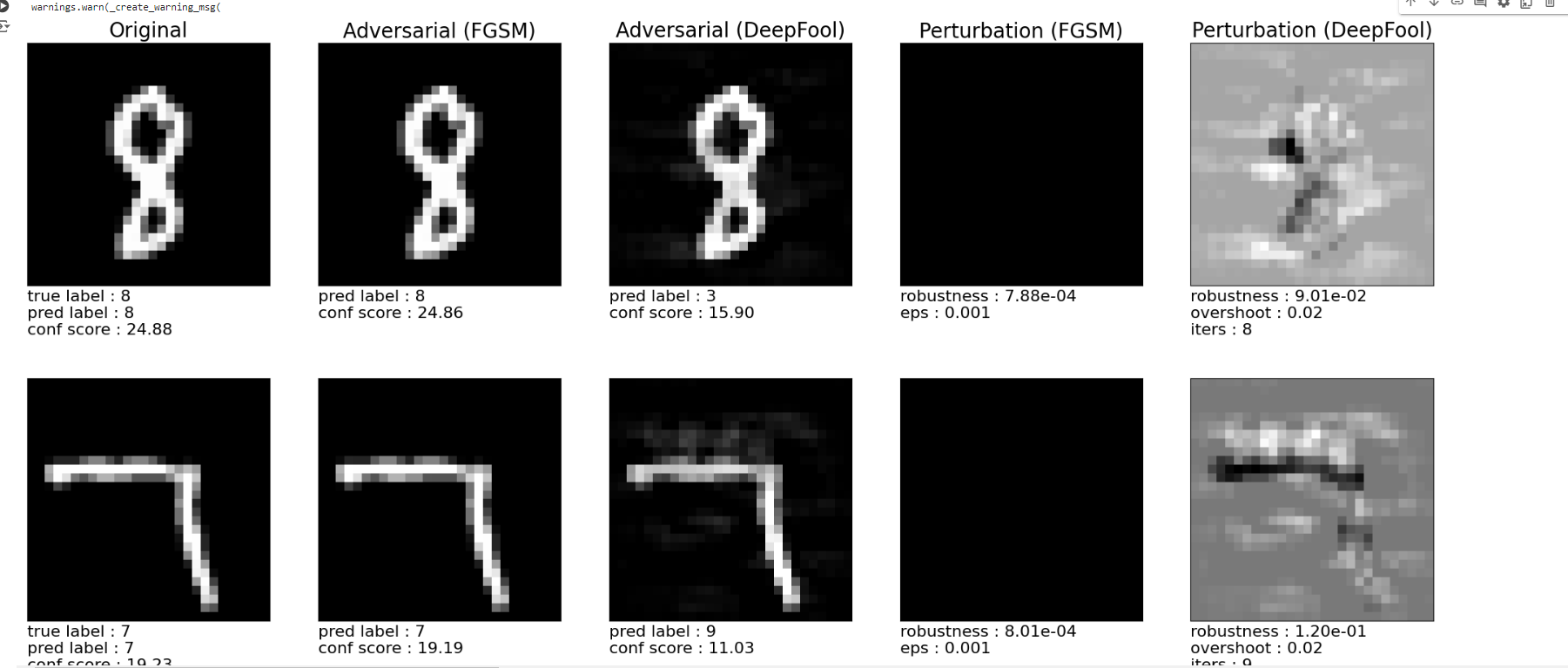
**FC MNIST** 

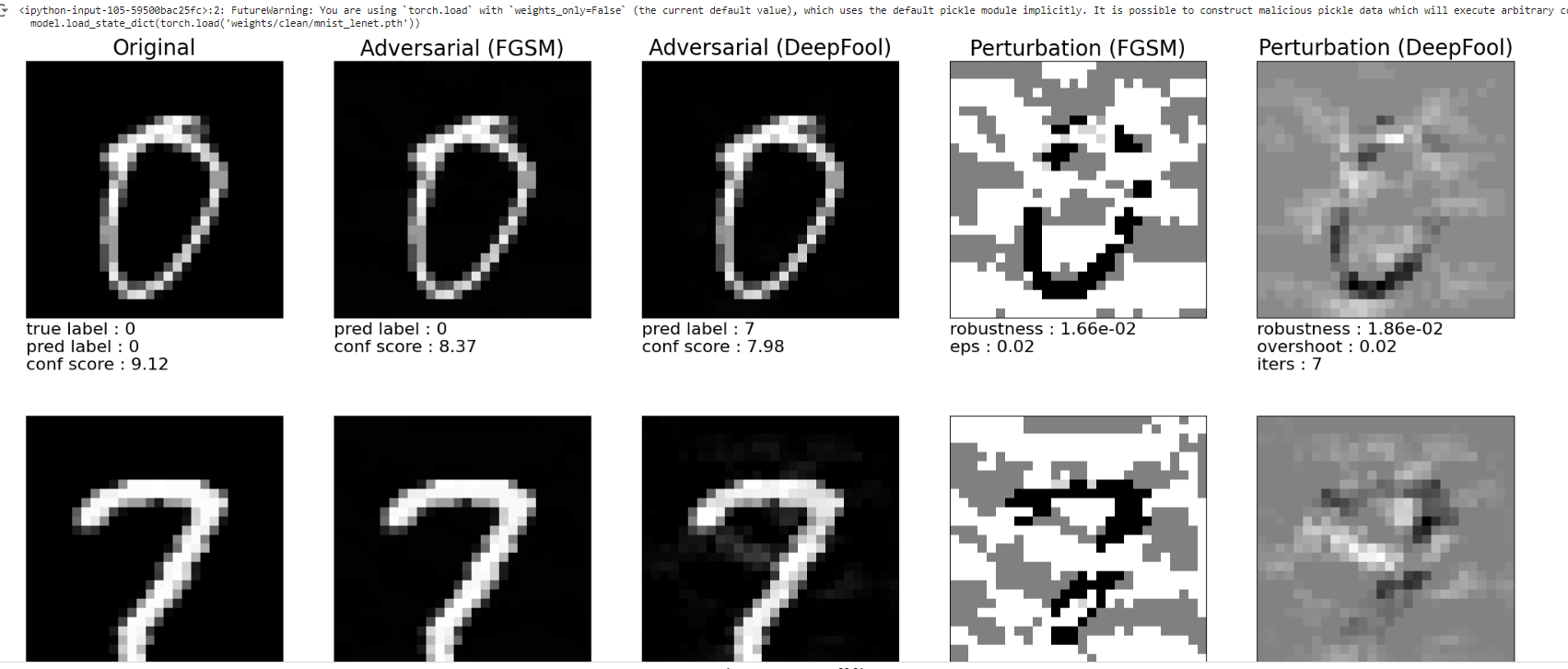
**Network-In-Network CIFAR-10** 

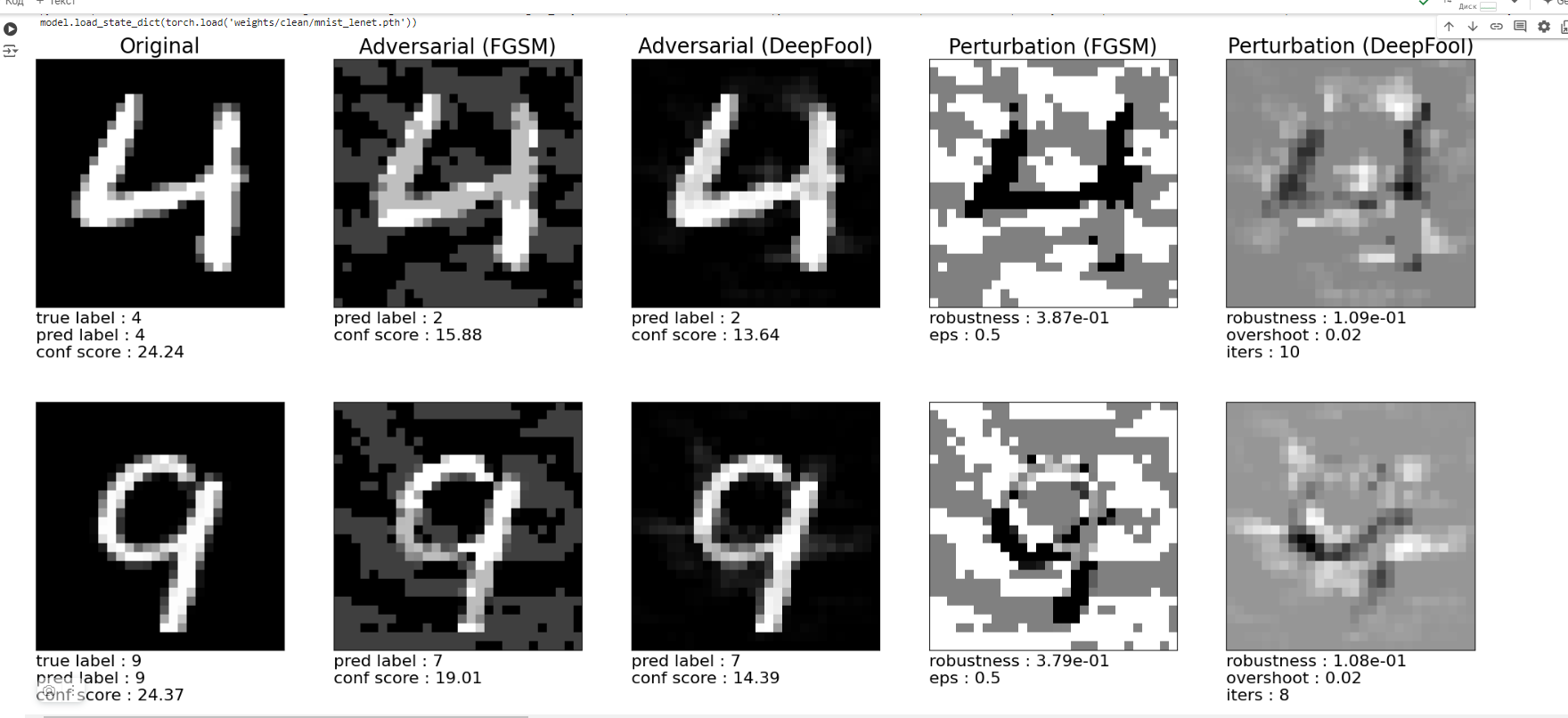
**LeNet CIFAR-10** 

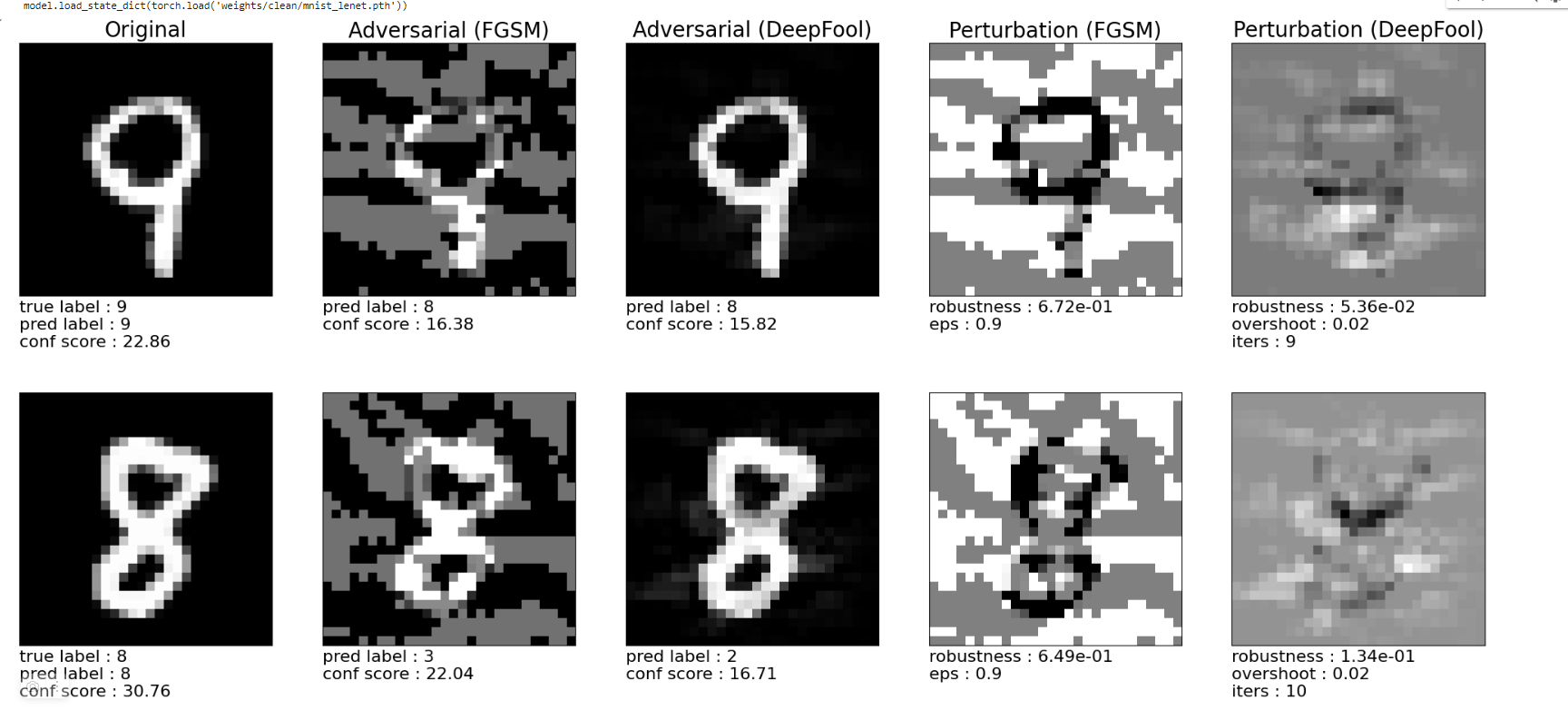
**Визуальное представление**

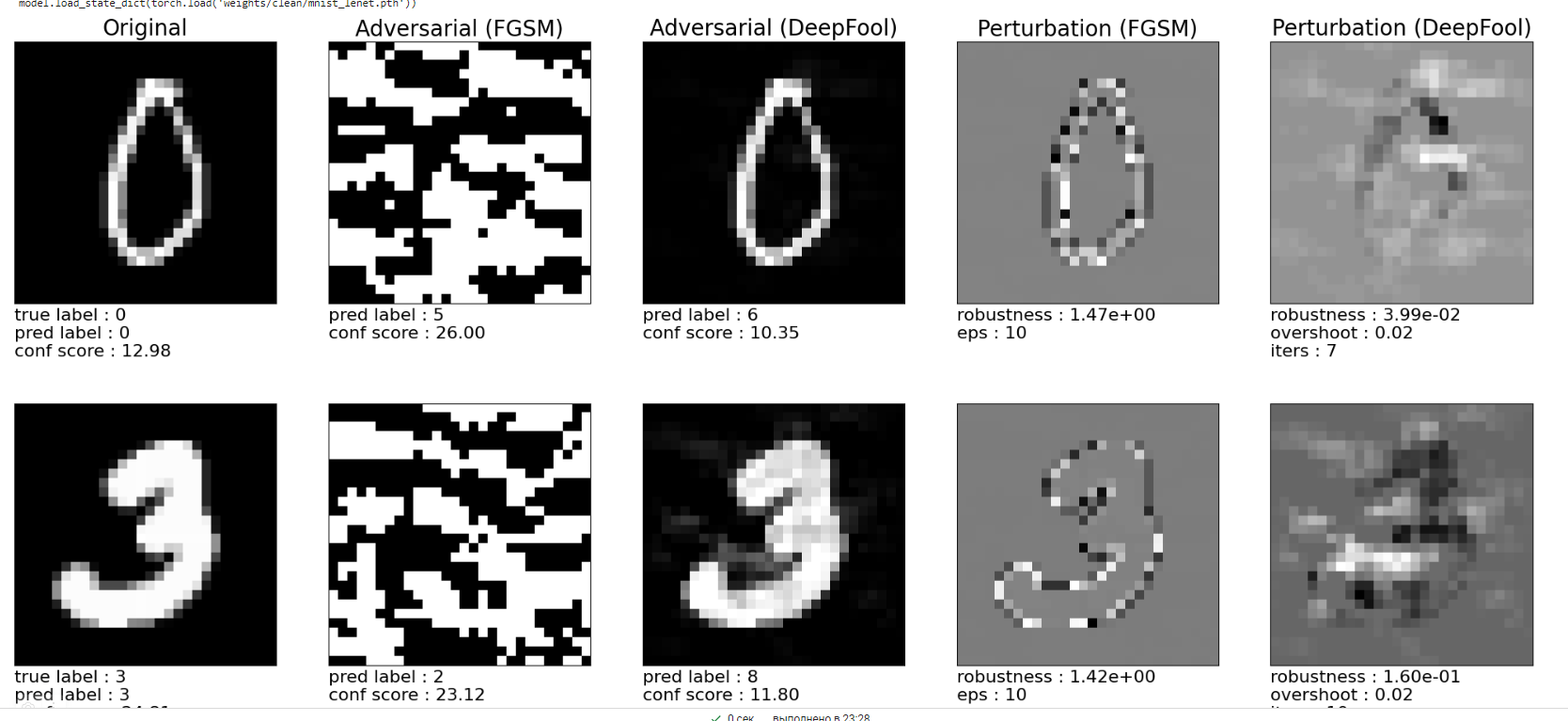
**LeNet MNIST**

fgsm\_eps = 0.001 

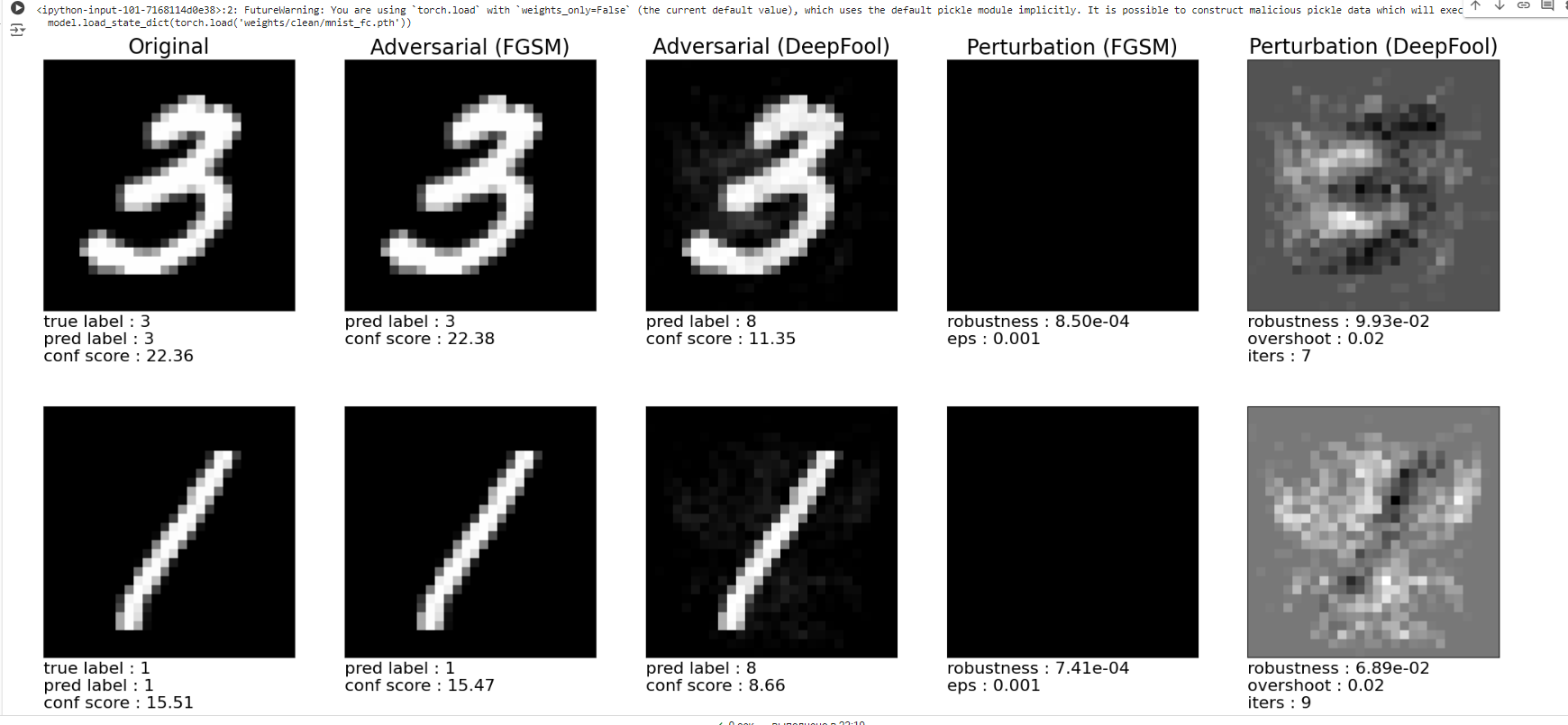
fgsm\_eps = 0.02 

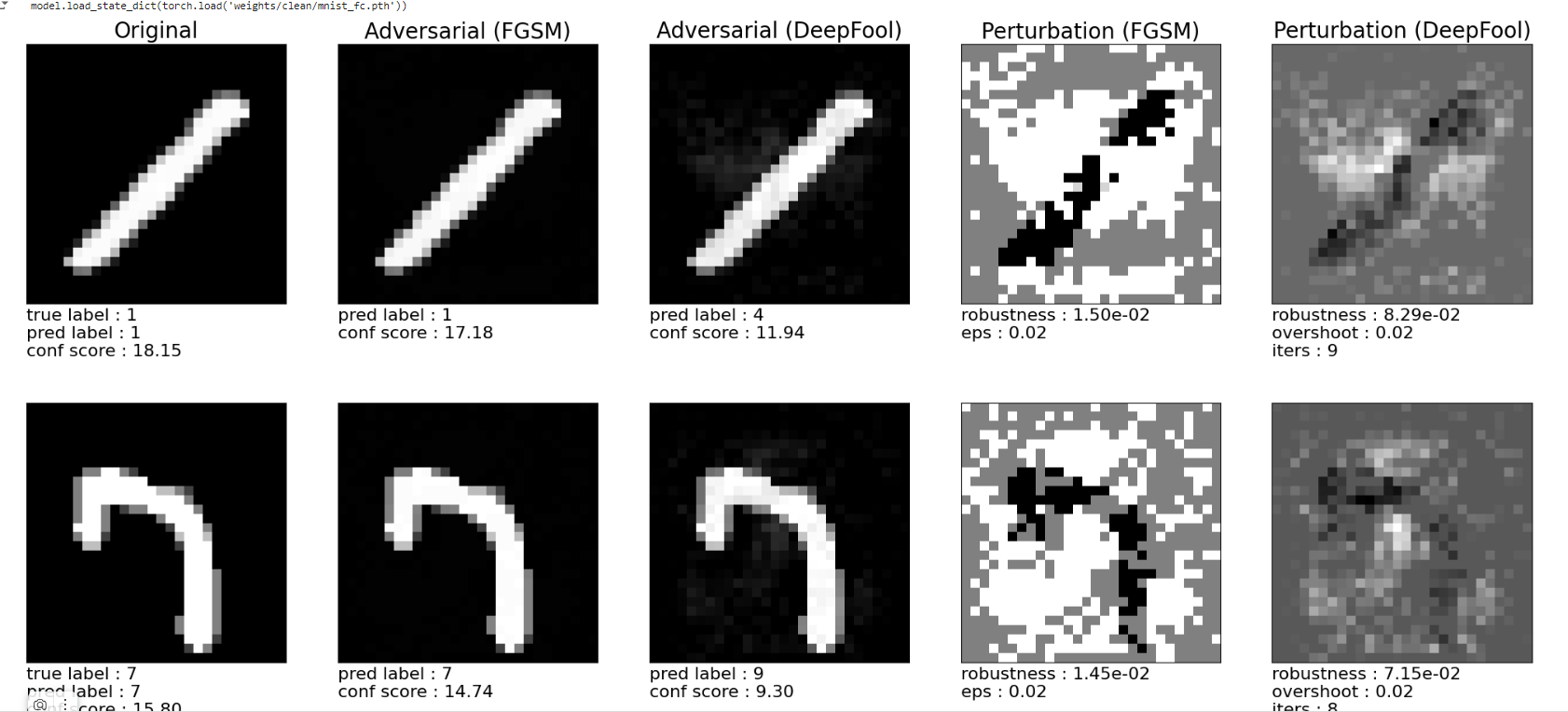
fgsm\_eps = 0.5 

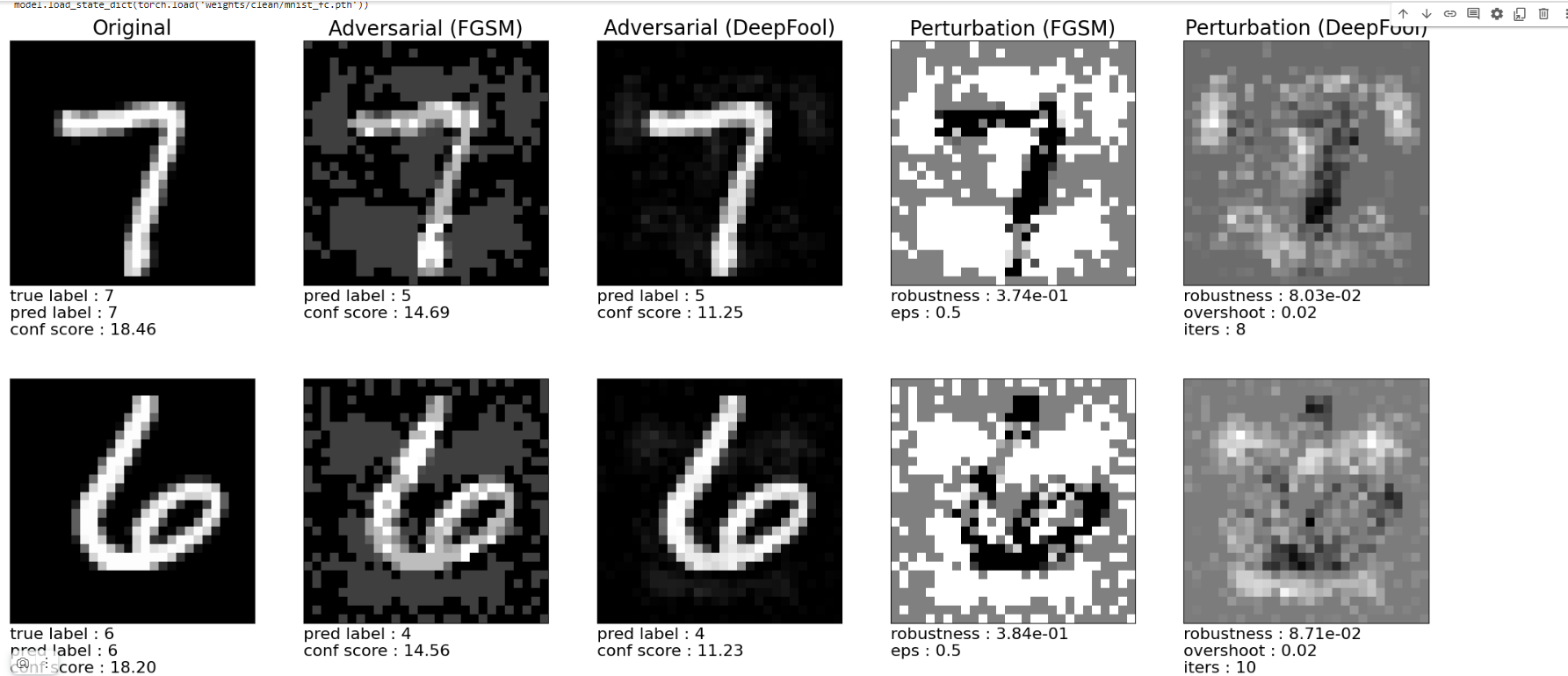
fgsm\_eps = 0.9

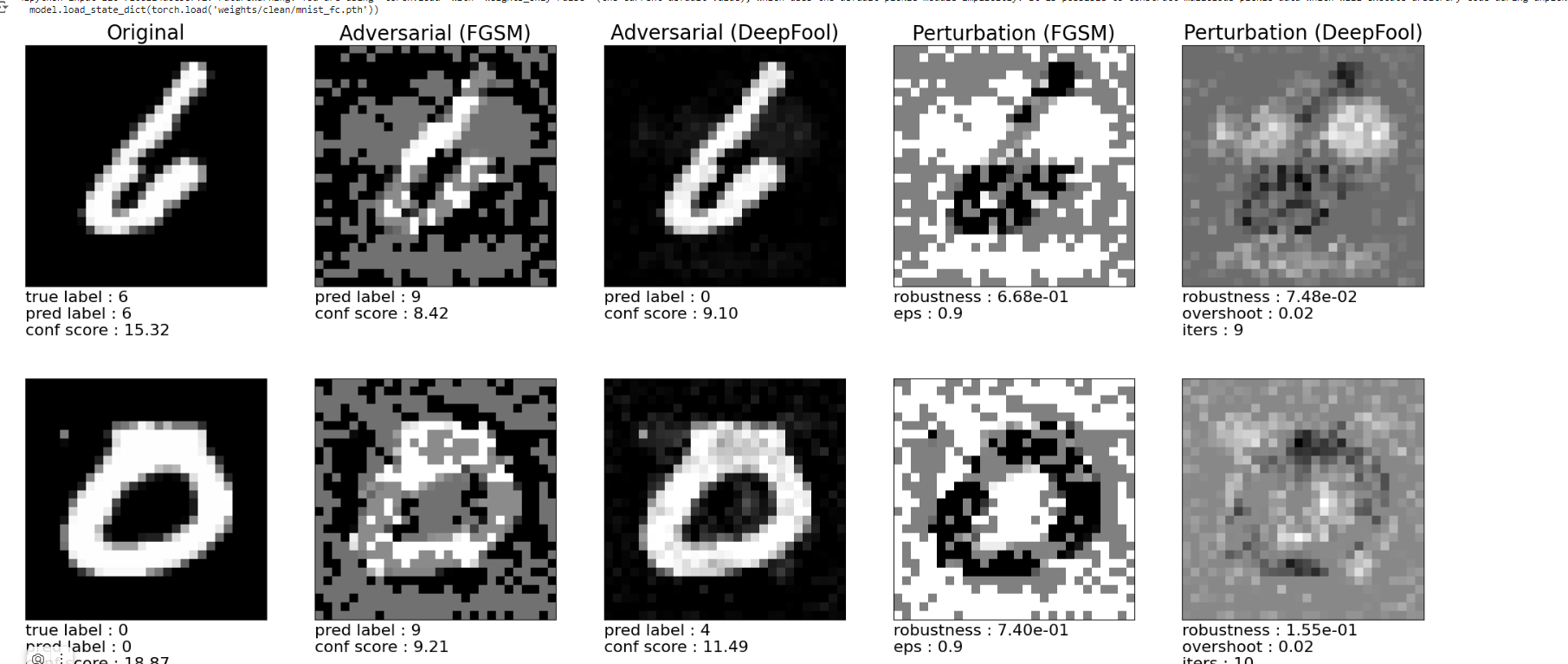
fgsm\_eps = 10

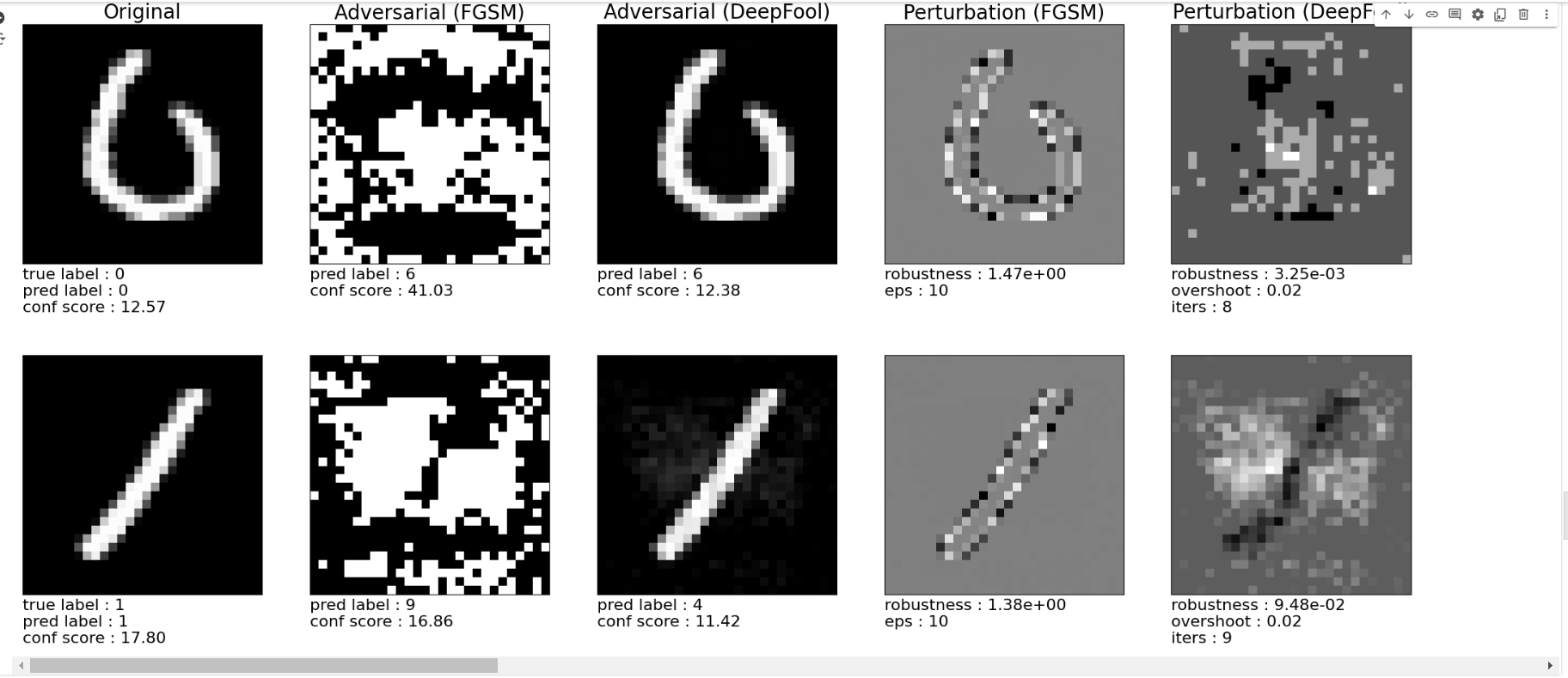
**FC MNIST**

fgsm\_eps = 0.001 

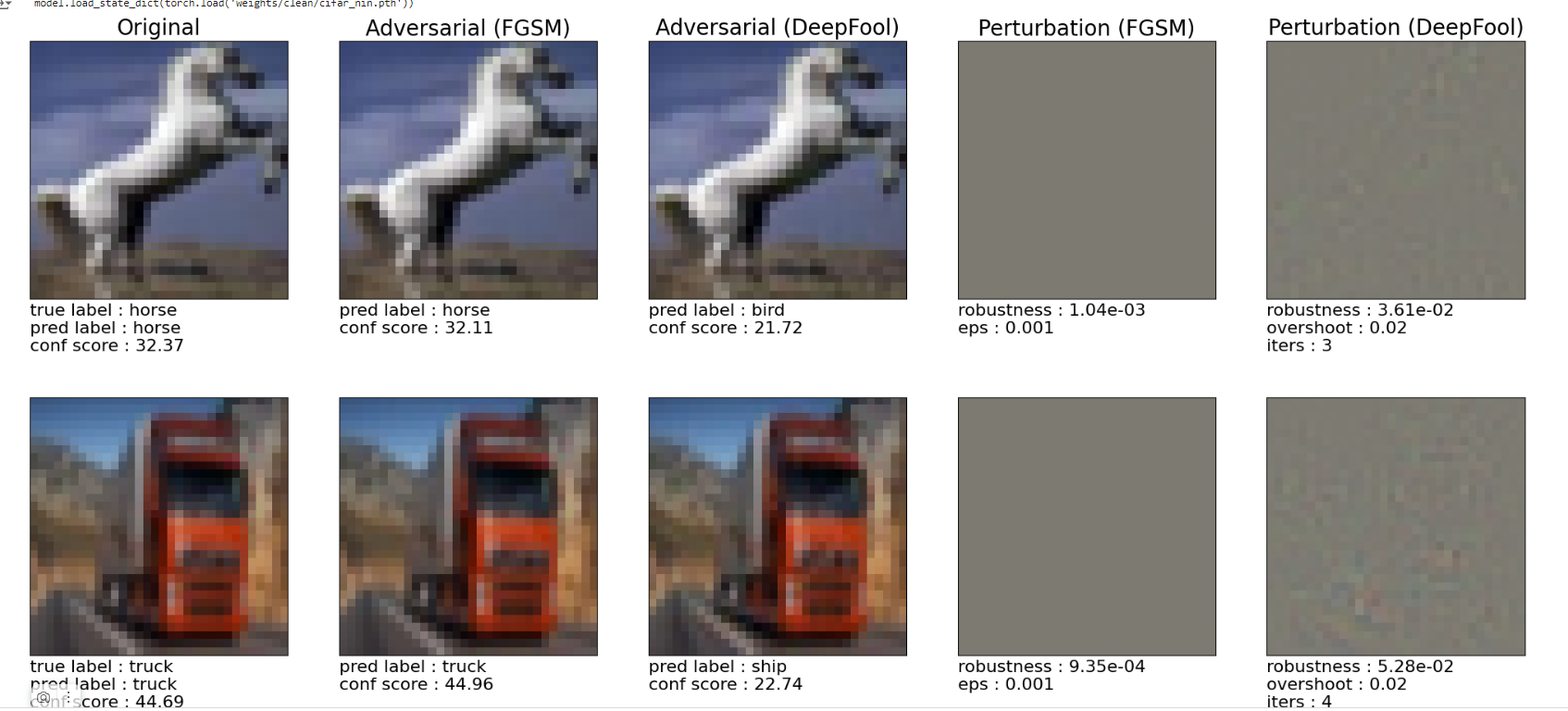
fgsm\_eps = 0.02

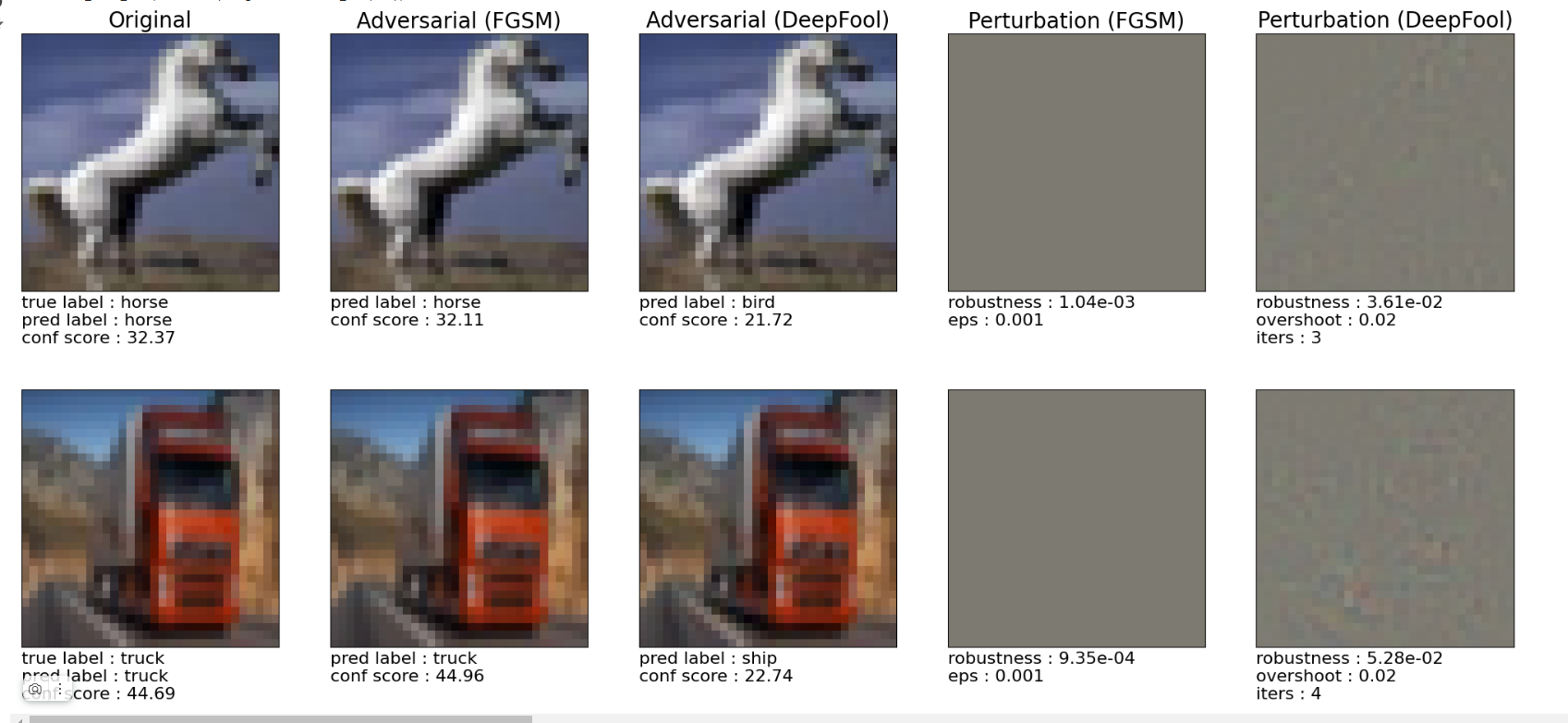
fgsm\_eps = 0.5

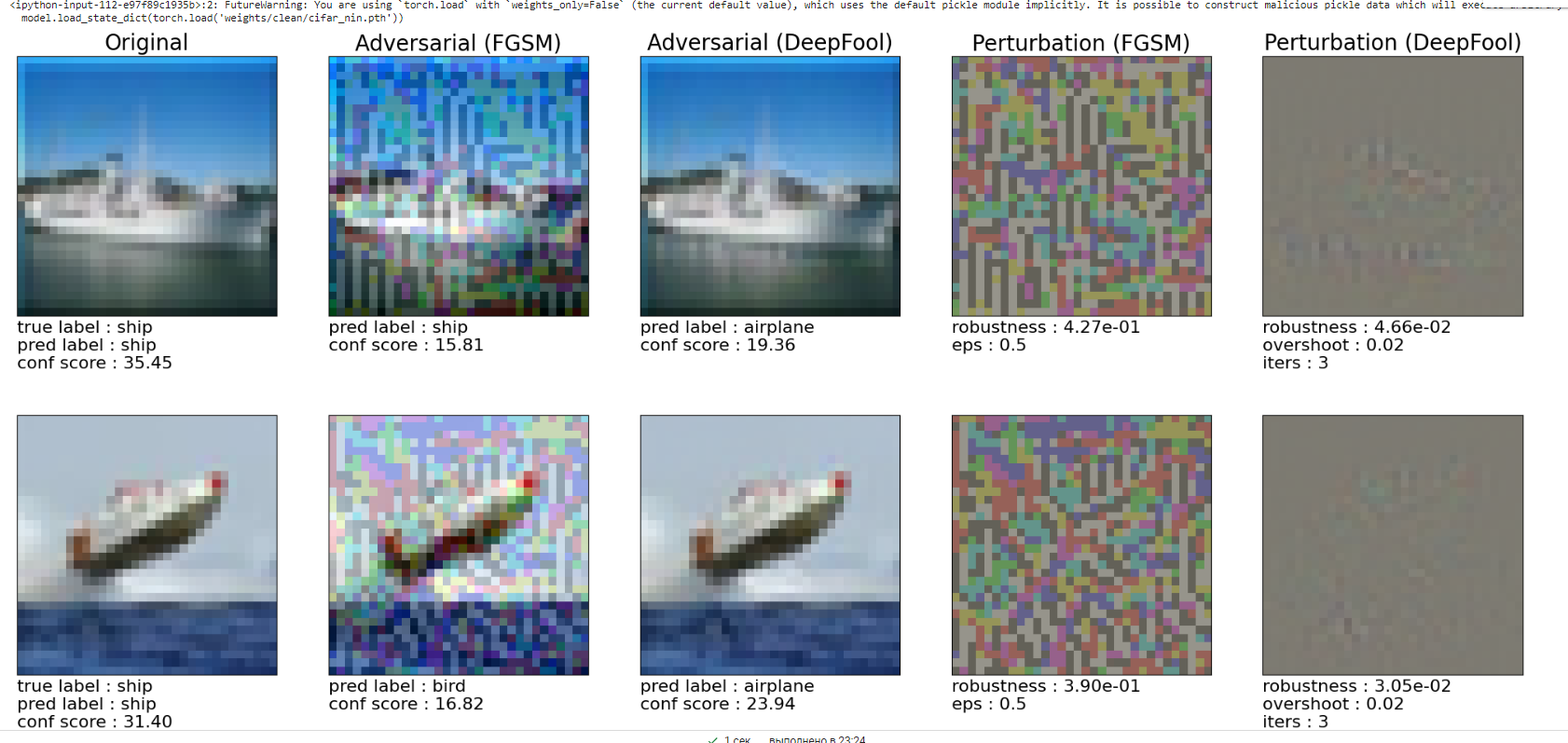
fgsm\_eps = 0.9

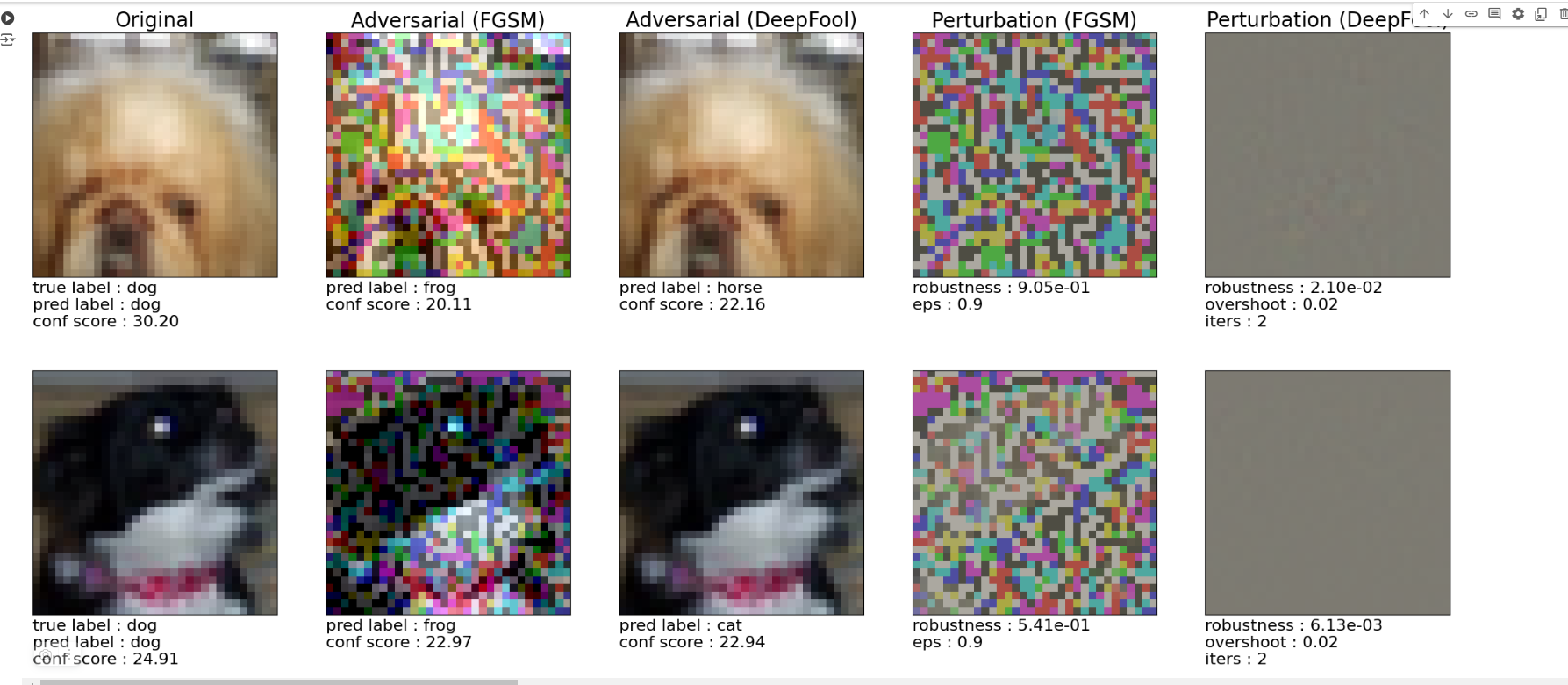
fgsm\_eps = 10

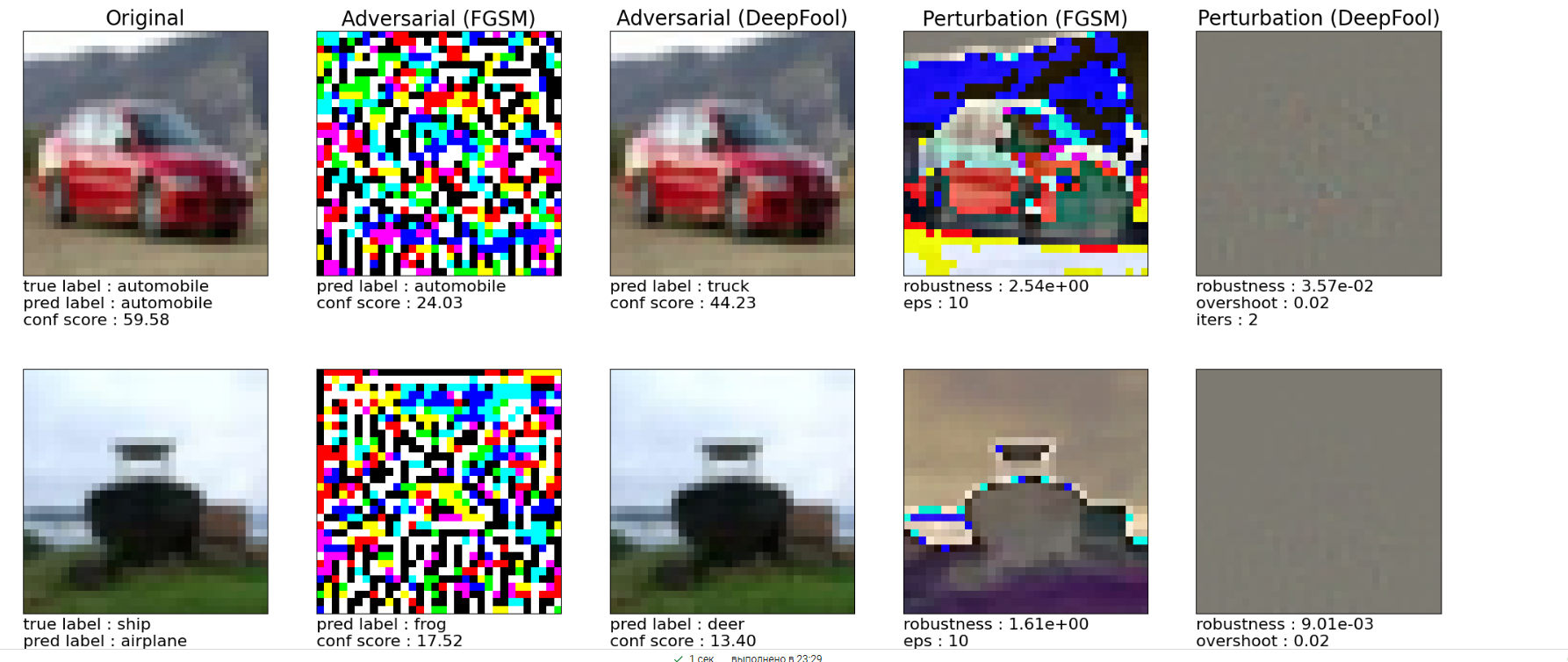
**Network-In-Network CIFAR-10**

fgsm\_eps = 0.001 

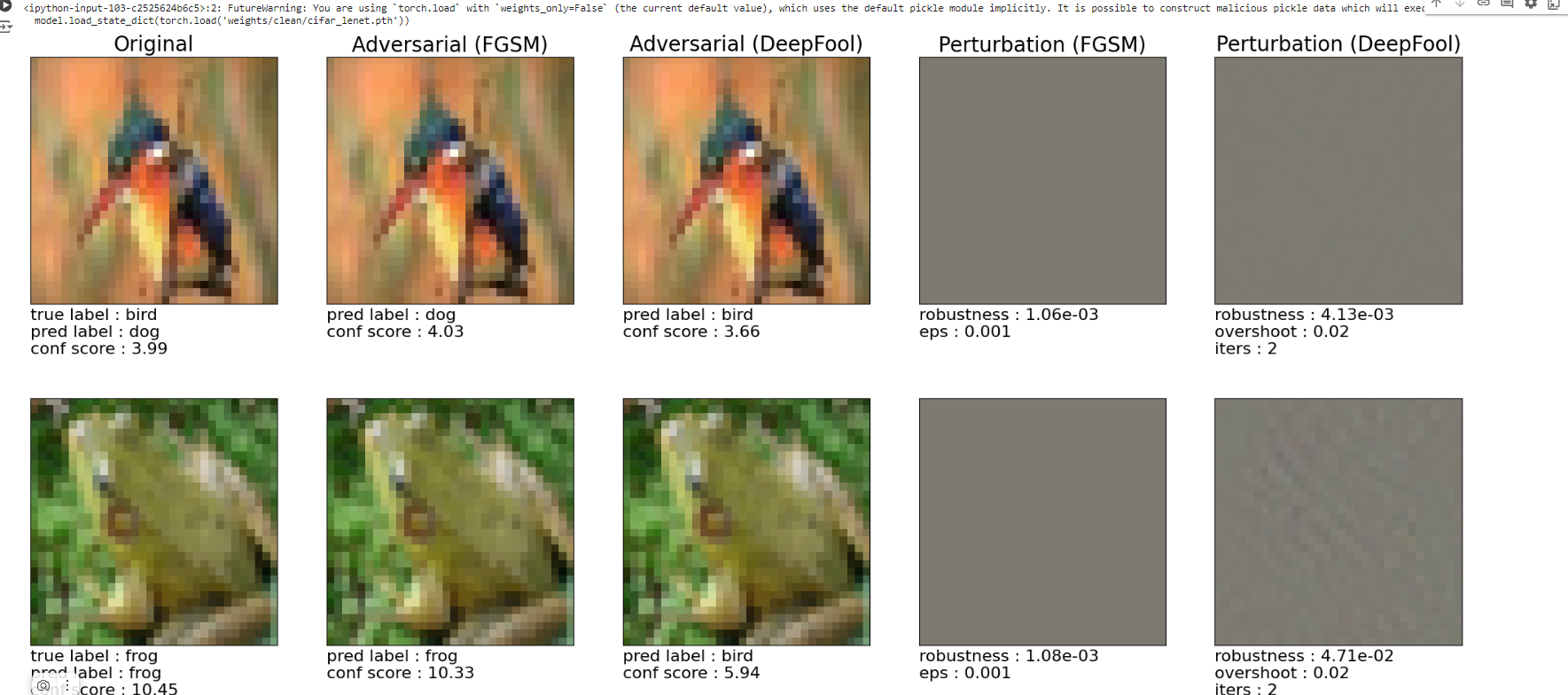
fgsm\_eps = 0.02 

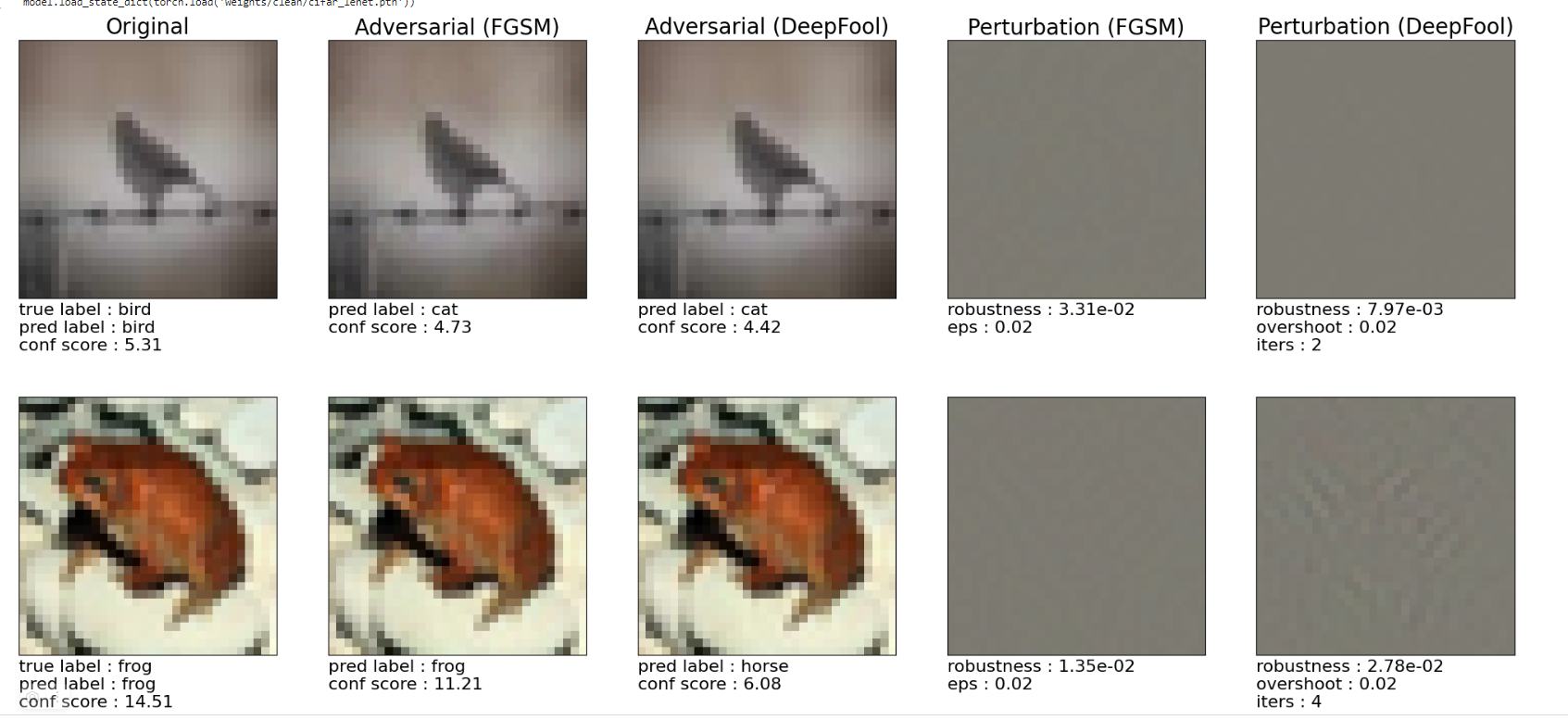
fgsm\_eps = 0.5

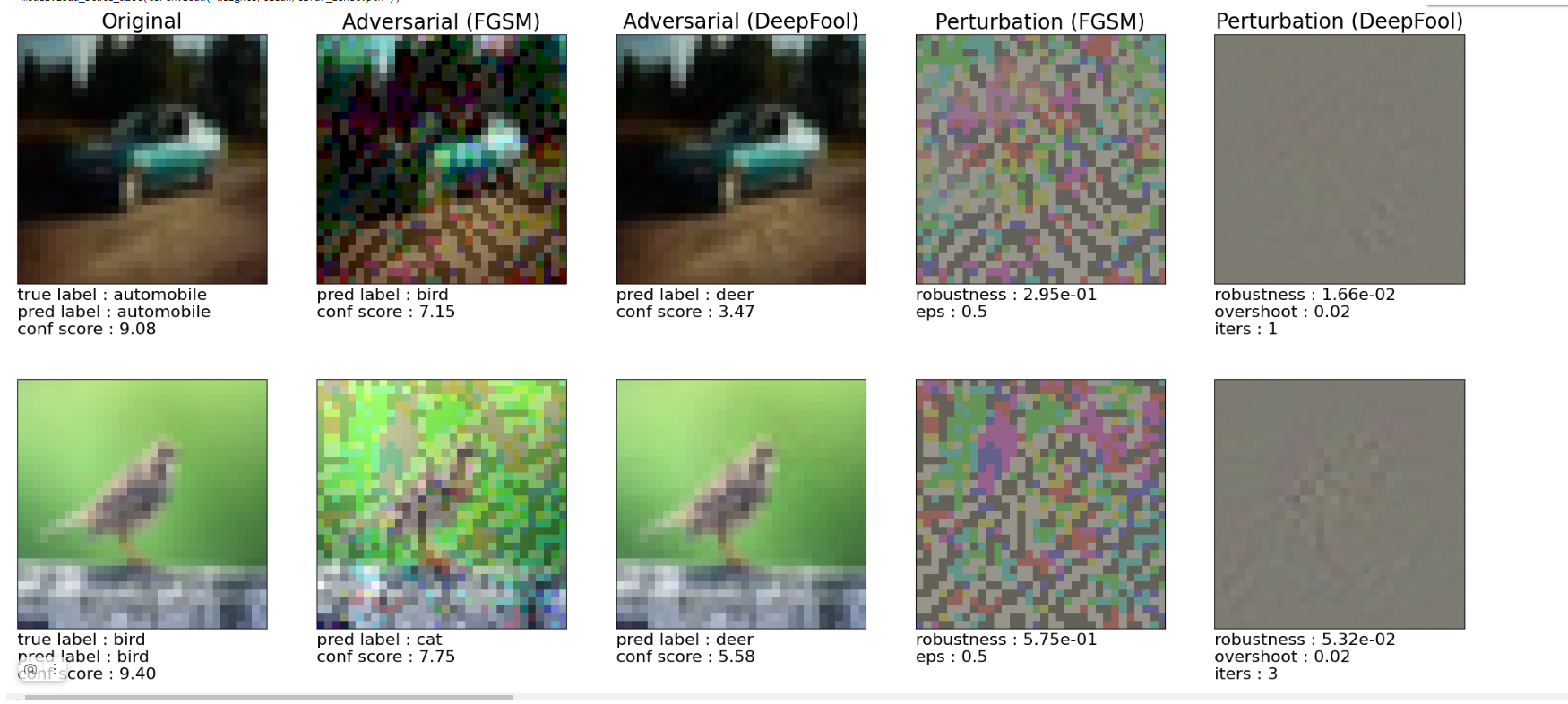
fgsm\_eps = 0.9

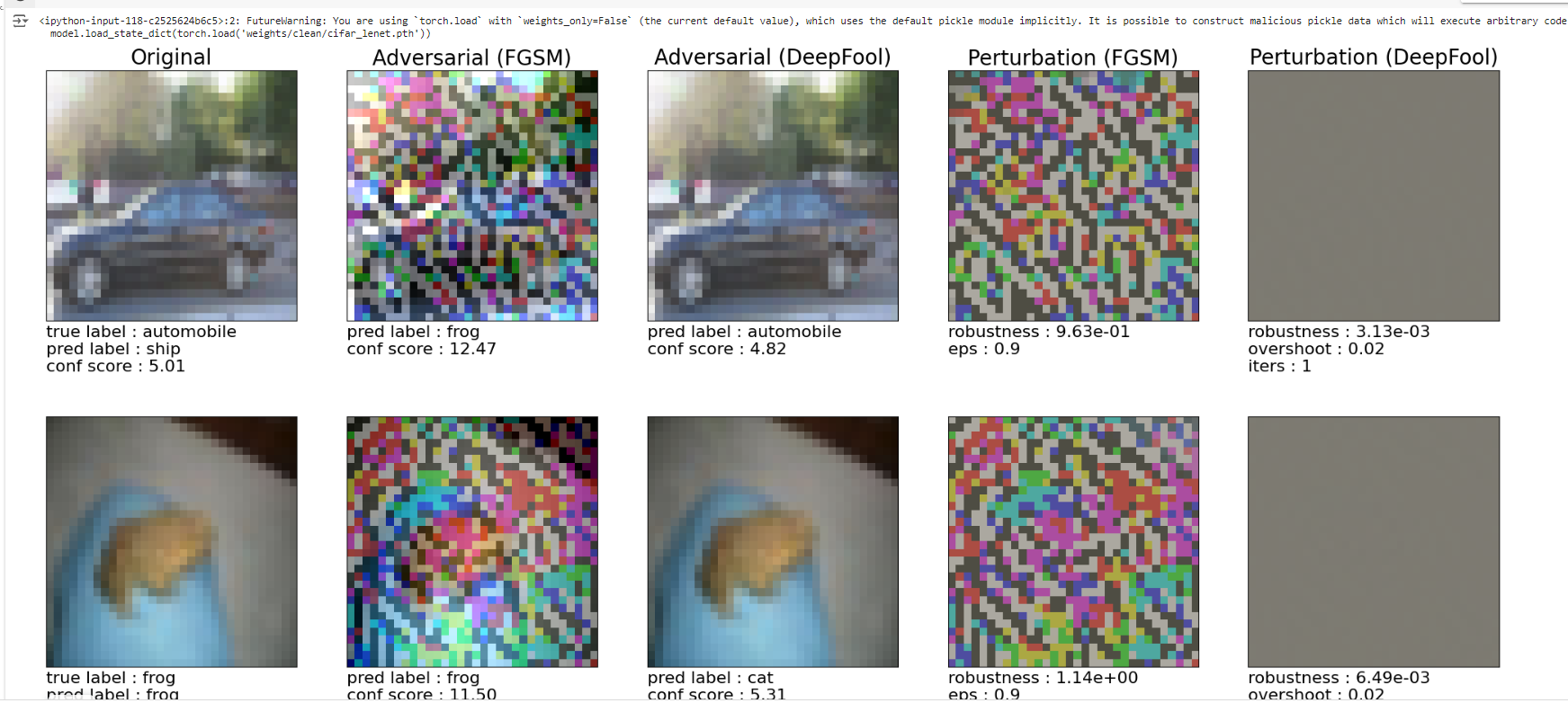
fgsm\_eps = 10

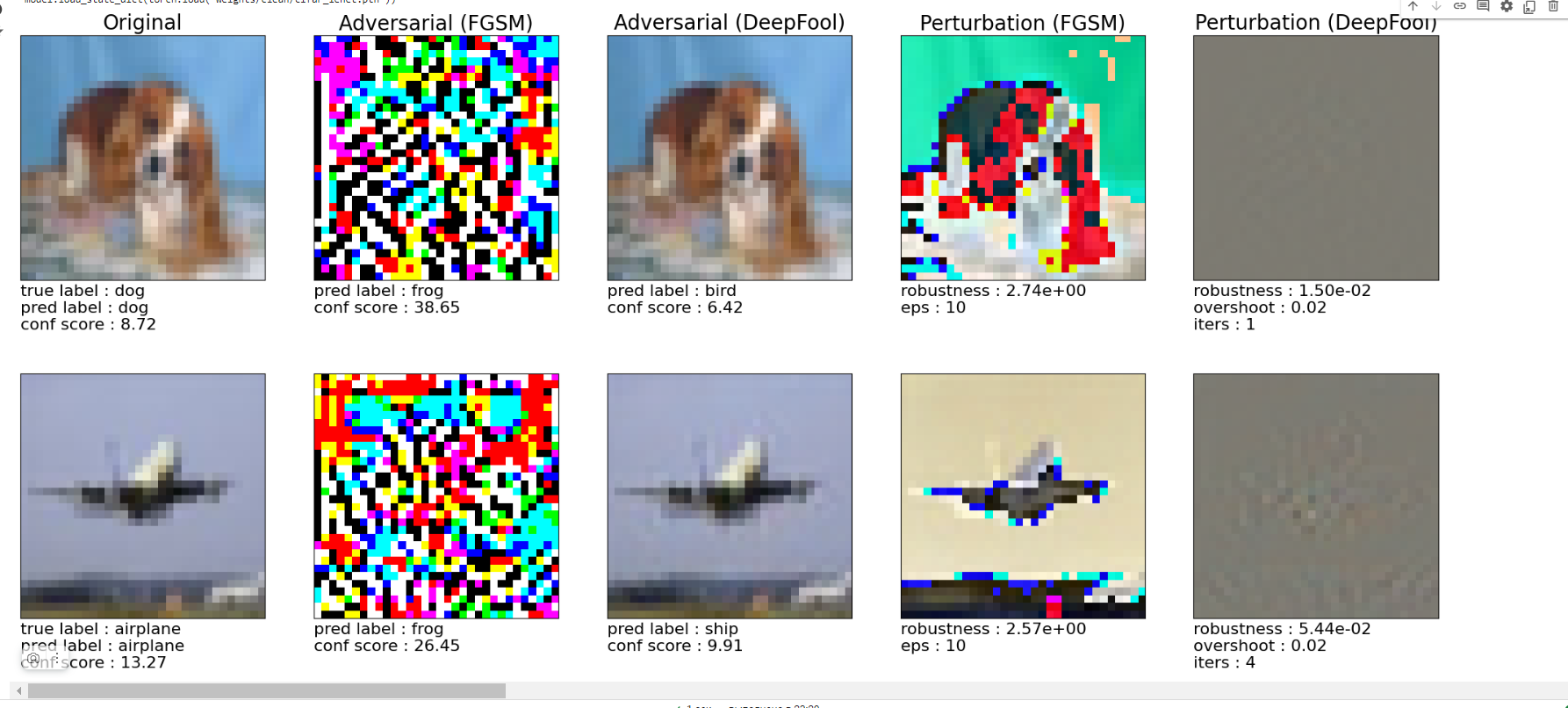
**LeNet CIFAR-10**

fgsm\_eps = 0.001 

fgsm\_eps = 0.02 

fgsm\_eps = 0.5

fgsm\_eps = 0.9

fgsm\_eps = 10

**Заключение**

Когда fgsm\_eps увеличивается, сети становятся уязвимее к атакам. Значительно уязвимее они становятся со значения fgsm\_eps = 0.5