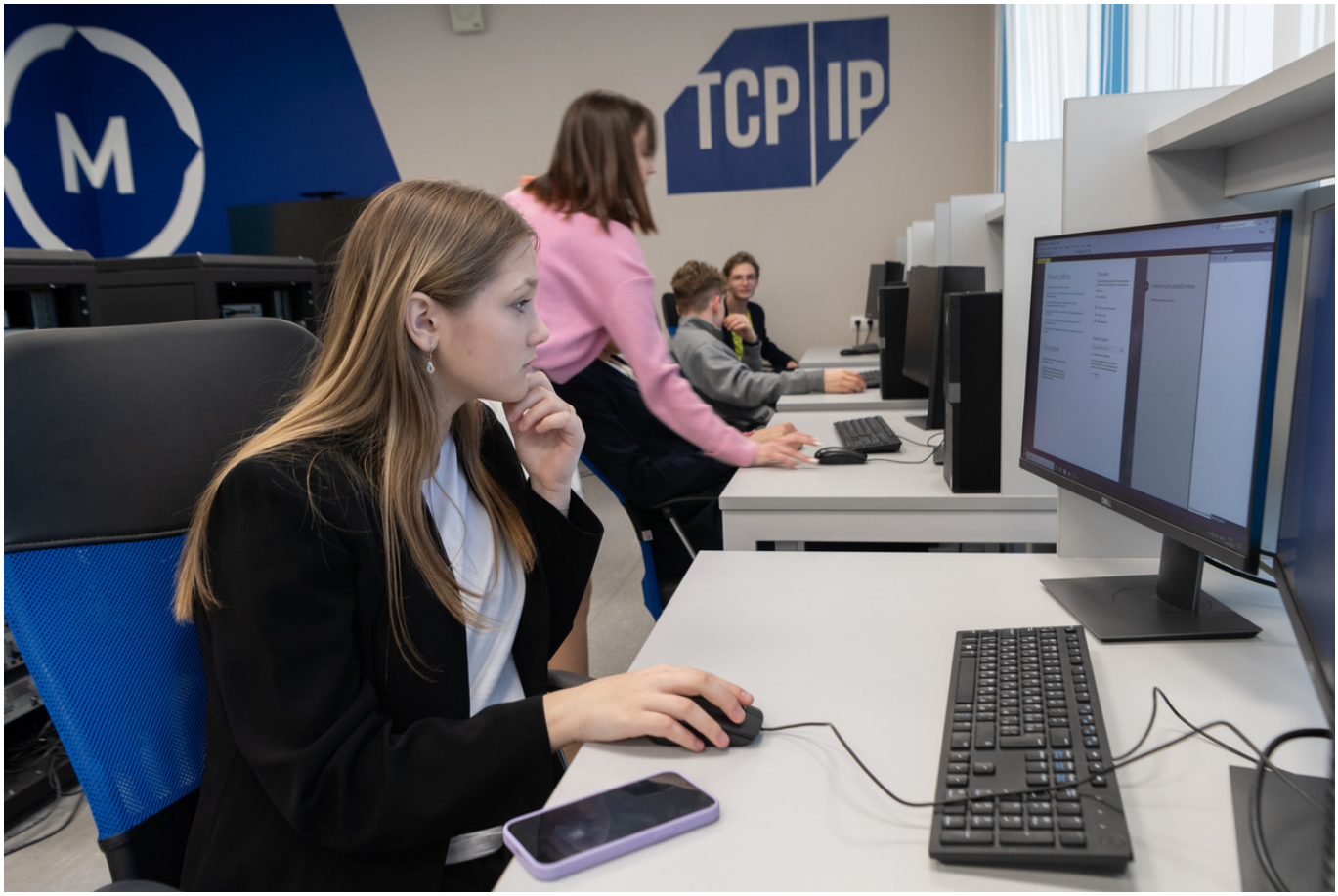
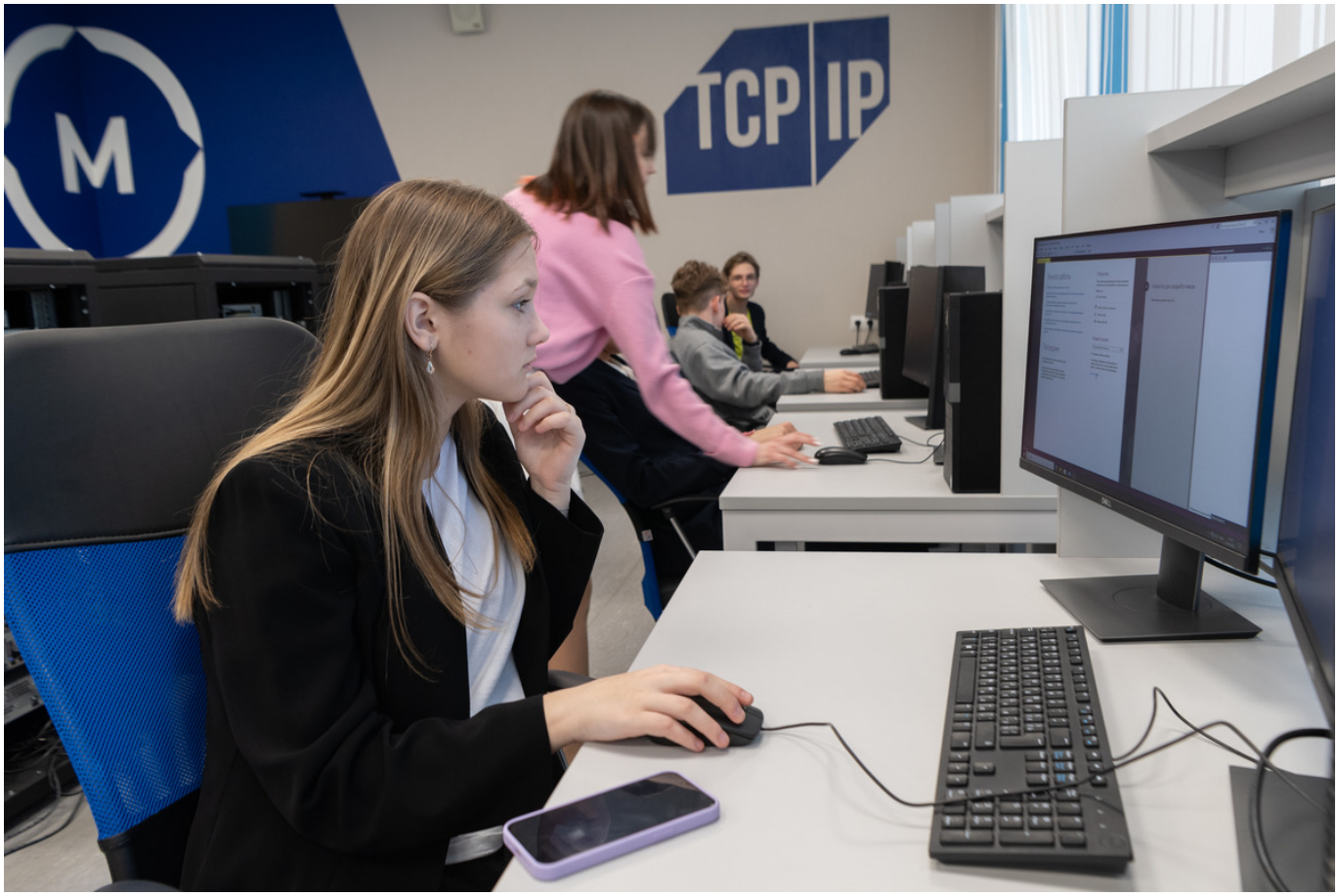
Учёные Политеха научили нейросеть бороться с мошенничеством в интернете



Учёные Политеха научили нейросеть бороться с мошенничеством в интернете

Учёные из Института кибербезопасности и защиты информации СПбПУ создали модель графовой нейронной сети, которая способна отличать подозрительные транзакции от безопасных, а мошенников — от честных пользователей. На экспериментальных испытаниях модель показала высокий потенциал. Научная статья с результатами исследования, проведённого в рамках программы «Приоритет-2030», опубликована в SpringerLink.



Графы — это структуры данных в виде сетей с парными связями внутри, они представлены как узлы и линии. Графовые нейронные сети ориентированы на работу со структурой графа. Учёные Политеха изучили графовые нейросети в банковской сфере.

«Мы представили банковские операции и пользователей, которые их совершают, в виде графов, затем разделили их на два класса: одни — мошенники, другие — люди, осуществляющие легитимные денежные переводы. При обучении графовой нейронной сети мы дополнительно учитывали идентификационную информацию: номер банковской карты, данные об отправителе и получателе денежных средств, тип используемой банковской карты, характеристики устройства, с помощью которого была совершена транзакция и другие», — поделилась д. т. н., профессор ИКиЗИ Дарья Лаврова.

Главное оружие новой модели нейронной сети в том, что она уделяет внимание определенным закономерностям, по которым можно распознать противоправные действия. При «фильтрации» транзакций, например, нейросеть смотрит на временные метки, по которым определяет, как давно человек стал участником банковской среды и в какой организации обслуживается. Учитывает она и изменения в сумме денежных переводов, и информацию об источнике транзакции.

Разработка Политеха способна экономить человеческий ресурс, автоматизирует рутинную работу по ручному разбору транзакций, которую выполняют сотрудники банков. Им останется разобраться только с теми операциями, которые нейронная сеть сочла подозрительными. И работая с нейросетью, организации не будут тратить бюджет на перенастройку сетевой инфраструктуры, закупку средств информационной безопасности, обучение сотрудников правилам так называемой «цифровой гигиены», а самое главное — на компенсацию ущерба от мошенников.

«Обеспечение кибербезопасности — непрерывный процесс, вечная „гонка вооружений“ между технически квалифицированными специалистами по безопасности и нарушителями. Поэтому любая система защиты, скорее всего, рано или поздно будет взломана, но на смену ей будут созданы новые защитные механизмы. Мы работаем в направлении совершенствования нашей модели графовой нейронной сети, собирая и генерируя новые обучающие наборы данных, которые будут включать и более „хитрые“ транзакции», — отметил д. т. н., директор ИКиЗИ член-корреспондент РАН Дмитрий Зегжда.

Графовая нейронная сеть может использоваться в разных сферах, где данные представляют в виде набора объектов и связей между ними. Так, например, она справится с выявлением в социальных сетях пользователей, распространяющих дезинформацию или же с обнаружением сетевых атак в сетях передачи данных.