

Нейросети становятся объектами кражи по нескольким причинам, среди которых стремление устраниить разрыв с конкурентами, кража личных данных и ускорение процесса создания новых моделей. Эту информацию предоставил Олег Рогов, руководитель научной группы «Доверенные и безопасные интеллектуальные системы» в Институте искусственного интеллекта AIRI.

Один из основных мотивов воровства заключается в желании обогнать конкурентов или достичь технологического преимущества. Кража нейросетей также позволяет сократить время, затрачиваемое на разработку архитектуры, обучение и тестирование моделей.

Кроме того, доступ к украденным моделям может означать получение конфиденциальной информации, например, банковских данных или биометрических параметров, обрабатываемых этими системами. Эту проблему отметил специалист в области кибербезопасности.

Чтобы выявить факт кражи нейросети, часто используются цифровые водяные знаки, которые помогают отслеживать и защищать интеллектуальную собственность от несанкционированного доступа.