АНАЛІЗ ЗАСТОСУВАННЯ ГЕНЕРАТИВНО-ЗМАГАЛЬНИХ МЕРЕЖ У СФЕРІ КІБЕРБЕЗПЕКИ

Ляшенко О.С., Щербина Д.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті передумови виникнення генеративно-змагальної мережі (GAN), її архітектури та концепції основ безпеки системи, розглянуті найсучасніші методи захисту безпеки, які були налаштовані за допомогою GAN.

Об'єктом дослідження є спектр різних застосувань GAN у сфері кібербезпеки. Предмет дослідження – методи та підходи застосування GAN в атаках на інформаційні системи та їх запобігання.

GAN є відносно новою технологією, тому дослідження додатків безпеки на основі цієї технології також почалися нещодавно [1]. Застосування GAN для безпеки можна розглядати як дуже потужний крок вперед і цінний інструмент для аналізу та застосування до проблем кібербезпеки. На сьогодні GAN показали перспективу у створенні нових методів захисту у сфері кібервторгнення, виявлення зловмисного програмного забезпечення та захищеної стеганографії зображень, хоча відповідні дослідження були обмеженими. З точки зору атаки на безпеку, багато доступних досліджень було зосереджено на створенні шкідливих програм для IDS. Нові генеровані атаки або зловмисне програмне забезпечення надають інформацію про раніше невідомі атаки і, таким чином, допомагають оновити механізми захисту.

У роботі розглянуті останні дослідження GAN від стеганографії зображень і нейронної криптографії до генерації зловмисного програмного забезпечення з метою навчити систему краще захищатися під час несприятливих сценаріїв атак. Показані різні дослідницькі можливості для поєднання генеративно-змагальних мереж із кібербезпекою.

У роботі проведений аналіз різних типів і варіацій GAN, які використовувалися дослідниками для вирішення значущих сценаріїв безпеки [2]. Докладно розглядається використання GAN для покращення спостереження в таких сферах, як протоколи безпеки та посилення систем виявлення для боротьби з конфіденційністю даних, роботи над створенням кращої системи виявлення вторгнень, безпечної стеганографії зображень, нейронної криптографії та аналізу безпеки.

Список літератури

1. I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio «Generative Adversarial Networks» NIPS'14: Матеріали 27-ї Міжнародної конференції з нейронних систем обробки інформації, 2014, с. 2672–2680.

2. H. Chen, L. Jiang «Efficient GAN-based method for cyber-intrusion detection» arXiv, 2019.