Конференция «Неделя науки Института кибербезопасности и защиты информации СПбПУ».

На базе Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого прошла «Неделя науки ИКиЗИ», национальная научная конференция для студентов, аспирантов и молодых исследователей. С 27 по 30 июня докладчики «Недели науки ИКиЗИ» обсуждали киберугрозы и противодействие им в рамках 31-й всероссийской конференции МиТСОБИ.

Молодежная секция, на которой представляли доклады «Недели науки ИКиЗИ», по количеству участников стала самой массовой на конференции. Молодые ученые обратили свой научно-исследовательский взгляд на наиболее актуальные и важные вопросы кибербезопасности. На секции обсуждали методы защиты систем ИИ и машинного обучения, современные модели и методы выявления киберугроз, технологии киберустойчивости и управления безопасностью.

Докладчики исследовали распространение информации в социальных сетях и механизмы защиты сверхточных искусственных нейронных сетей, разбирались с проблемами безопасности java-приложений, офисных документов, искусственного интеллекта и социальных сетей, представляли собственные разработки.

И.В. Кришталь, В.С. Давыденко, А.В. Первушин и Д.В. Нагибин из Военно-космической академии имени А. Ф. Можайского разработали, например, программный комплекс

защищенного обмена текстовой и мультимедийной информацией «Агат», а С.В. Шевченко, О.Р. Бурнаев и С.Ф. Ткаченко из этого же учебного заведения – сервис установления источников и путей распространения деструктивной информации в социальных сетях. Их разработка сама собирает и обрабатывает данные, из которых потом извлекает признаки негативного контента и дополняет их возрастом «агрессоров», лайками и подписками. Пока сервис работает только с сетью Twitter, но планируется расширять его функционал.

Многие из тем, поднятых на секции, либо уже играют, либо в скором времени будут играть определяющее значение для безопасности пользователей. Э.Р. Сабиров (ВМиК МГУим. М.В. Ломоносова) и Г.Б. Маршалко (Академия криптографии Российской Федерации) рассказали об использовании генеративно-состязательных сетей для защиты изображений от автоматической классификации. При публикации в интернете все фотоснимки и картинки классифицируются и индексируются поисковыми службами, что потенциально может угрожать приватности юзеров. Ограничить доступ к данным поможет построение и публикация состязательных изображений – они визуально схожи с оригинальными, но некорректно классифицируются алгоритмами распознавания. Получить их можно как раз с помощью генеративно-состязательных сетей (GAN) – архитектуры из двух нейронных сетей (генератора и дискриминатора), настроенных на работу друг против друга.

Из-за необходимости обработки большого числа данных использование систем машинного обучения в последние годы стало практически повсеместным. И.А. Кобрин, А.В. Вишняков и А.Н. Федотов из ИСП РАН коснулись вопроса безопасности фреймворков машинного обучения, а Е.А. Рудницкая и М.А. Полтавцева из Санкт-Петербургского политехнического университета Петра Великого рассмотрели и систематизировали существующие атаки на системы машинного обучения, проанализировали методы защиты и апробировали их на примере атак уклонения.

Активно продолжается процесс расширения векторов атак, используемых злоумышленниками – он требует внедрения новых технологий анализа в элементы защиты для отслеживания спектра угроз. Эту нишу занимают технологии искусственного интеллекта: их довольно широко применяют в задачах обнаружения аномалий в сетевом поведении и выявления подозрительной активности. А.В. Хабибуллин, А.В. Гомон и С.С. Андрушкевич из Военно-космической академии имени А.Ф. Можайского описали использование злоумышленниками искусственного интеллекта, придя к выводу о необходимости применения дополнительных средств защиты.

Е.И. Ткачева и М.О. Калинин из Санкт-Петербургского политехнического университета

Петра Великого разобрались с выявлением киберугроз в системах интернета вещей, технология которого становится неотъемлемой частью информационной инфраструктуры общества. Из-за быстрого роста и количества подключаемых устройств она предоставляет всё больше возможностей нарушителям безопасности. Для защиты сетевых инфраструктур используют системы обнаружения вторжений. Ученые рассматривали подход многоагентного обучения с подкреплением для реализации обнаружения нарушений безопасности в системах Интернета вещей. От обычной многоагентная система отличается тем, что в среде функционирует не один агент, а несколько. Исследователями разработаны и реализованы три типа многоагентного обучения с подкреплением: полностью децентрализованное, с передачей информации о прогнозах, с передачей информации о наблюдениях.

По широкому спектру тем заметно, что кибербезопасность необходима совершенно разным областям и может быть реализована множеством технологий и разработок. Их развитию и расширению способствует участие в теоретических и практических исследованиях молодых ученых с новым взглядом на привычные проблемы.

Со всеми тезисами можно подробнее ознакомиться в материалах конференции