СТОИТ ЛИ ОПАСАТЬСЯ НЕЙРОННЫХ СЕТЕЙ

Бауыржан Алибек Нурбекулы

студент, кафедра информатики Костанайский региональный университет имени А. Байтурсынова, Казахстан, г. Костанай

Изучая тему нейросетей, не сложно задаться вопросами «будущие или конец света?», «заменит ли нейросеть человека?» и «настал ли скайнет?»

Не для кого не секрет, что нейросеть стремительно набирает популярность. Нейросеть это схожая с нейронными сетями человека математическая модель, которая имеет програмное или аппаратное воплощение. Нейросеть – это попытка воплотить в реальность научно фантастическую мечту о искусственном интелекте с помощью моделирования сетей на подобии человеческого мозга. После того как людям удалось придумать алгоритмов обучения, эти машины научились делать определенные прогнозы, распознавать и заменять лица на фото или видео, выполнять задачи управления и распознание картинок, видео и аудио файлов. Человеческий мозг содержит около 65 миллиардов нейронов, каждый из которых имеет около сотни синапсов. Кроме того, нейроны являются довольно интересным объектом изучения, поскольку не все нейроны работают по одной и той же формуле. Существует около 100 типов нейронов. Однако перед исследованием вопросов Нейросети, строение головного мозга человека — это ряд определённых проблемы. Первая проблема – это то что, очень сложно с моделировать. Вторая проблема, эта модель очень сложно распланировать, так как мозг человека очень схож своеобразным суперкомпьютером, все нейроны мозга человека работают параллельно друг другу. нейросети уже везде, а для жизни им всего лишь нужен хороший процессор, как в привычных для нас персональных компьютеров. Этот искусственный интеллект уже водит машины за нас, учитывая все правила дорожного движения, поверхность дорог, плотность движения, скорость и соседние машины. А на это, на минуту, лучше, чем некоторые люди. Шанс того, что вы попадете в ДТП минимальный. Автопилот на машинах на столько продвинут, что он без каких-либо проблем сможет увернуться от кошки, которая выбежала на проезжую часть.

Помимо всего, нейросеть неплохо развлекает интернет. Если вы когда-нибудь задумывали о том, как бы выглядел тот или иной человек, вместо какого-нибудь актера в большом кино, то теперь это не проблема. неросеть способна заменить лица людей без каких-либо проблем, система deepfake способна заменять лица на столько, что иногда очень сложно отличить где настоящий фрагмент, а где работа нейросетей. Она может повторить любую мимику лица и не только. Помимо видео эта тема также может сделать так чтобы человек говорил то чего никогда не говорил. Эта система может делать искусственную замену аудио файлов видео файлов и фото. Эта система анализирует внешность человека, его голос и с помощью самообучения делает своеобразный вывод о том, как разговаривает как двигается человек, его мимику движения и тембр голоса. Для этого используются две Нейросети, одна из них генерирует изображения, а вторая находят различия с оригиналом. Такая система предназначена для того чтобы вырастить могла самосовершенствоваться, добиваться идеалы собственно недели. Deepfake работает с открытыми алгоритмами машинного обучения и работает вместе, чтобы обеспечить высочайшее качество контента. Нейронная сеть получает изображения из библиотеки и обучается с помощью видео с сайтов видеохостингов. В то же время искусственный интеллект сопоставил фрагменты оригинального портрета с содержанием видео, в результате чего получился разумный материал.

Так в чем же все таки опасность неросети?

Услышав много полезных вещей о нейросети, вы все же можете задаться вопросом «а в чем же опасность нейросети?».

Как нам известно, что уже в 2017-м году постепенно стали появляться поддельные видео. Изначально, всё это выглядело весьма безобидно и даже забавно. Все поддельные видео были в основном любительскими видео, которые были созданы с помощью бесплатных инструментов OR, в которых были лица знаменитости, наложенные на порнографические материалы. Но спустя Некоторое время эта технология стала развиваться весьма быстро, из-за чего теперь очень сложно распознать где оригинал, а где фэйк.

Таким способом было устроенная первая информационная атака из-за дип фэйка. Современные аналитики говорят, что эта технология может стать самый опасный в цифровом пространстве за последние десятилетия. Теперь люди опасаются, что эта технология может привести к использованию как оружие против отдельных лиц. Для примера, в 2018-м году была опубликована большего видео бывшим президентом США Бараком Обамой. В этом видео он якобы оскорблял нынешнюю главу государства Соединённых Штатов Америки.

Как оказалось, Видео было сделано с помощью программ в бесплатном пользовании. Следующий фэйковый инфо повод случился после публично обрисован у вас состояния о персональных данных всех людей от Марка Цукерберга. Как оказалось, видео так же было опубликовано с помощью Нейросети. После всего этого с каждым днём появляется все больше фэйковые новостей которые могут повлиять на репутацию компаний и государства и бороться с этим очень сложно, так как отличить подделку стало очень сложно.

Современные хакеры имеют мало общего с образом одиноких профессионалов, представленным в телесериале. Хакеры, занимающиеся незаконной деятельностью, по большей части являются частью организованных преступных групп, часто объединенных большим количеством программистов относительно низкого уровня.

Как и в любой организованной преступной группе, их главная цель-получить прибыль с минимальными затратами и риском. Это определяет основное направление работы киберпреступников: большинство преступлений, которые они совершают, связаны с кражей персональных данных пользователей, мошенничеством и вымогательством.

В результате существует пять основных типов киберугроз.

Более половины киберугроз-это зараженные компьютером вредоносные программы. В дополнение к вирусам, которые часто встречаются на веб—сайтах, хакеры уже давно используют более интересные методы-например, встраивание вредоносного кода в проекты с открытым исходным кодом или заражение серверов для автоматического обновления программного обеспечения.

В последнем случае десятки (а возможно, и сотни) тысяч компьютеров по всему миру заражаются через такие системы.

Другой тип-это атака на личное мошенничество. Они означают прямой контакт с пользователем, чтобы убедить его отказаться от данных или добровольно установить приложение, содержащее вредоносный код. В таких атаках обычно участвуют реальные люди, которые могут притворяться службами поддержки, банковскими служащими и так далее.

Такие нападения часто связаны с прямым хищением денег. Иногда результатом атаки является заражение вирусом закодированных данных и необходимость перевода средств для их разблокировки (это виртуальная форма вымогателей).

Классический взлом системы с помощью программ, скриптов и т.д. На этот вид преступлений приходится менее 17% всех киберугроз.

Обычно это часть глобального сценария—например, заражение сервера вредоносным ПО. Одной из основных целей взлома (в дополнение к традиционным государственным институтам) являются криптобиржи и другие платформы, связанные с криптовалютами.

Атаки на веб-сайты по-прежнему популярны. В основном речь идет об интернет-магазинах и других сайтах, которые накапливают личную информацию своих пользователей. Эти данные либо просто украли, либо использовали схему вымогателей.

Наконец, последний тип-это не устаревшая DDoS-атака. В июле 2019 года им только что исполнилось 20 лет. Основная идея здесь заключается в создании бот-сети-команды, готовой отправить запрос на данный сервер, перегрузив его компьютер.

Несколько израильских исследователей решили выяснить, какой наибольший ущерб медицинским учреждениям могут нанести хакеры. С этой целью они предлагают сценарий, при котором хакеры могут получить доступ к личным данным пациентов, особенно к рентгеновским снимкам, через уязвимые программные продукты.

Предположим, хакеры используют обученные нейронные сети для выполнения совершенно особой задачи: "удалить" раковые опухоли с помощью рентгеновских лучей. По словам исследователей, такое вмешательство в персональные данные может иметь фатальные последствия для пациентов.

Подобных статей довольно много, но, как и в этой статье, они не учитывают многих факторов.

Прежде всего, нейронные сети, упомянутые в этом исследовании, могут быть созданы только с участием большого числа экспертов и должны быть обучены на основе данных, полученных в ходе конкретного медицинского исследования. Вы не можете ожидать, что обычная хакерская группа будет иметь доступ к таким учебным образцам.

Во-вторых, описанный сценарий означает очень дорогую и очень специальную атаку на данные. Как ни странно, в статье говорится об изменении изображения, но других записей, таких как анализы пациентов, нет. Это означает, что сами авторы работы, возможно, значительно упростили сложность придуманной ими атаки, предназначенной для вмешательства в медицинские данные, чтобы повлиять на диагноз.

Поэтому большинство экспертов сходятся во мнении, что в этом нет ничего удивительного: для текущих задач взлома существующие нейронные сети не подходят из-за высокой сложности и стоимости обучения. Если возникнет новая угроза, связанная с нейронными сетями, это произойдет только с новыми методами, которые их используют.

Значит, хакерам не нужны нейронные сети?

Вредоносное ПО может нанести значительный ущерб производственным мощностям. В результате WannaCry-вирус, который изначально не предназначался для атаки на заводскую систему,-привел к закрытию производства на нескольких заводах Renault, а также вошел в производственную систему Nissan.

Другими словами, правильный ответ состоит из двух частей.

Прежде всего, обычным хакерам не нужны нейронные сети, но в промышленном шпионаже и атаках на государственном уровне они могут найти свое применение и даже нашли его.

Во-вторых, прогресс не будет стоять на месте. Если использование нейронных сетей сейчас является долгим и дорогостоящим, это не значит, что так будет всегда. С появлением стандартизированных библиотек наборы данных, помеченные общественным достоянием, могут значительно изменить эту ситуацию. Тогда использование нейронных сетей может войти в жизнь обычных пользователей. Поэтому сейчас необходимо рассмотреть эти угрозы.