ЭЛЕКТРОННАЯ СИСТЕМА ГОЛОСОВАНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Волков М.А.

Насуро Е.В. – к.т.н., доцент

Демократическоеголосованияявляетсяоднимизрешающих и, безусловно, серьезнымполитическим событием в любой стране. В настоящеевремя самый распространённый способголосования - черезбумажнуюсистему. Однако, насегодняшнийдень, такаясистема безнадежно устарела и требуетвнедрения более современных технологий. Системы электронного голосования позволяют ускорить процесс подсчёта голосов, а также упростить голосование людям с ограниченными возможностями.

Цифровое голосование - это использование электронных устройств, таких как машины для голосования или интернет-браузер, для подачи голосов. Голосование с использованием специальных устройств получило название «электронное голосование» (e-voting), а голосование с помощью интернет-браузера называют «интернет голосованием» (i-voting).

Системы электронного подсчёта голосов применяются на выборах с 1960-х годов, с тех пор, как появились перфокарты. Первые перфокарты и компьютеризированные машины для подсчета голосов использовались в Грузии в 1964 году, вскоре примеру последовало и США (в Орегоне и Калифорнии). Системы прямой записи голосов (DRE - Direct Recording Electronic), накапливающие голоса на одном устройстве, используются повсеместно в Бразилии, также достаточно широко распространены в Индии, Нидерландах, Венесуэле и США. Система голосования с прямой записью осуществляет сбор голосов путём предоставления механических или электрооптических компонентов (как правило, кнопки или сенсорные экраны), которые могут быть использованы избирателем. Информация о голосах накапливается на специальных носителях; после голосования она сводится в таблицы, хранимые на съёмных носителях, а также может быть распечатана. Также система может передавать итоги в центр голосования для сверки и подсчёта. Как и все машины для голосования, системы DRE увеличивают скорость подсчета голосов. Они также могут включать широкий спектр вспомогательных технологии для самых больших классов людей с ограниченными возможностями, позволяя им голосовать без потери анонимности своего голоса. Эти машины могут использовать наушники и другие адаптивные технологии для обеспечения необходимой доступности голосования.

Системы Интернет-голосования завоевали популярность и используются в правительственных выборах и референдумах в Великобритании, Эстонии и Швейцарии, а также муниципальных выборах в Канаде и партийных выборах в США и Франции. Интернет-выборы — один из способов электронного голосования, представляющий собой проведение части или полностью голосования на выборах и референдуме с использованием сети Интернет. В Эстонии электронное голосование проводится с 2005 года, а в 2007 она стала первой страной в мире, разрешившей голосование в режиме онлайн. На парламентских выборах 2015 года 30,5% голосов было подано в рамках интернет системы голосования (i-voting). Основой этой системы является национальная идентификационная карточка, которая предоставляется абсолютно всем гражданам Эстонии. Эти карты содержат зашифрованные файлы, которые идентифицируют владельца, и позволяют выполнять ряд онлайн и электронных мероприятий. Когда избиратель подает свой голос, он передается через общедоступный сервер подачи голосов в базу, где он будет храниться в зашифрованном виде, пока не закончится онлайн период для голосования. Затем из поданного голоса стирается вся личная информация избирателя, и все голоса переносят на сервер подсчета голосов, который не имеет доступа ни к одной сети. Сервер расшифровывает и подсчитывает голоса, а затем выводит результаты.

Основным минусом традиционных систем остается открытость и безопасность. В последнее время данные общественного мнения часто фальсифицируются для достижения различных политических, социальных и корпоративных целей. В связи с этим вопрос честного и открытого голосования стоит очень остро и требует современных и надежных способов решения проблемы. Электронное голосование подвержено хакерским атакам со многих сторон. Взломанное ПО может быть установлено как на машинах для голосования (личных устройствах либо специальных средствах), так и на центральных серверах подсчета голосов. Небезопасным является и процесс передачи данных по сети. Наличие единого сервера открывает возможность для осуществления DDoS и другого рода атак. Из-за сложности протоколов электронного голосования, потенциальных компьютерных ошибок и хакерских атак избирательные комиссии в Казахстане (2011) и Нидерландах (2008, 2017) возвращались к бумажным бюллетеням, урнам и ручному подсчету голосов.

Технология блокчейн решает многие проблемы безопасности, связанные с другими более традиционными системами голосования на основе общего единого сервера. Такая система позволяет создать прозрачные и надежные инструменты удаленного волеизлияния и сможет обеспечить защиту от внешнего воздействия на результаты голосования. Это форма распределенной базы данных, где записи принимают форму транзакций. Основная ценность блокчейн-цепи заключается в том, что она позволяет напрямую делиться базой данных без центрального администратора, вместо того, чтобы иметь некоторую централизованную логику приложения. Поскольку независимые участники системы, которые не могут доверять друг другу, должны подтвердить точность каждой транзакции и договориться о том, попадет ли

очередная запись в регистр или нет, она обеспечивает уровень прозрачности и постоянства, недоступный для традиционных способов голосования.

Разработка электронной системы голосования на основе технологии блокчейн позволило бы обеспечить прозрачность выборов, конфиденциальность информации избирателей, а также полную неприкосновенность и безопасность данных. Технология блокчейн обладает всеми характеристики, которые общественность ожидает получить от платформы, которая, возможно, является самой важной частью демократического общества.

Список использованных источников:

1. Andrew Barnes, Digital Voting with the use of Blockchain Technology
2. Roger Wattenhofer, The Science of the Blockchain : 2016
3. Springall, D., Security Analysis of the Estonian Internet Voting System : https://jhalderm.com/pub/papers/ivoting-ccs14.pdf : 25 сент. 2016

ПЕРЕНОС ОБУЧЕНИЯ ДЛЯ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гаврилович Ю.А.

Кобяк И.П. – к.т.н., доцент

Современные глубокие нейронные сети обладают интересным феноменом: будучи натренированными на большом количестве изображений, они все на первых слоях «выучивают» одинаковые шаблоны-фильтры или по-другому одинаковые приметы/признаки – простые линии, градиенты, углы, цветные пятна округлой формы. Присутствуют эти фильтры настолько часто, что отсутствие их при обучении нейронных сетей на не синтезированных наборах изображениях у опытных разработчиков вызывает подозрения в программных ошибках при разработке или обучении сети. Феномен проявляется на задачах обучения как с учителем, так и без.

Т.к. похоже, что нахождение/изучение таких одинаковых примет на начальных слоях нейронной сети не зависит от типа функции потерь (lossfunction) или от типа натурального (не синтетического) набора данных, то можно называть такие приметы *общими*. С другой стороны, мы знаем, что приметы, выученные на последних слоях натренированной сети, очень сильно зависят от используемого набора данных. Например, в сети с N-мерным выходным softmax слоем, которая была натренирована задаче классификации с учителем, каждый выходной узел будет специфичным для соответственного класса. Таким образом, приметы, выученные на последних слоях, можно называть *специфическими*.

Наличие *общих* и *специфических* примет так же хорошо согласуется с идеей иерархического обучения представлению, которая отражается в принципе работы глубоких нейронных сетей.

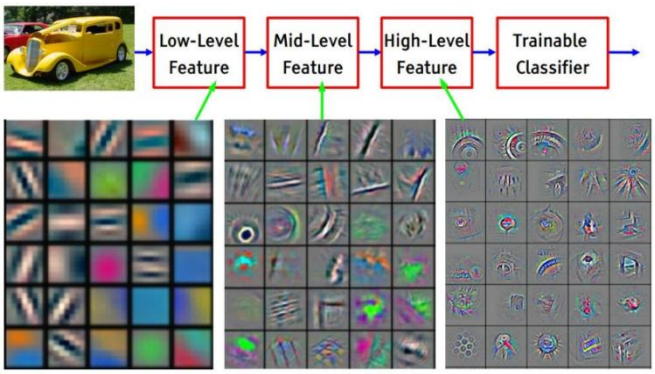

Рис. 1 – градация выученных фильтров от общих до специфических [1]

Почему нас интересует наличие *общих* или *специфических* примет? Потому, что если в процессе обучения нейронной сети можно выделить набор общих признаков, то далее мы можем использовать эти признаки для так называемого *переноса обучения* или *transferlearning* [2]. Для переноса обучения мы сначала тренируем *базовую* сеть на базовом наборе данных, затем мы переиспользуем выученные признаки, перенося их на вторую *целевую* сеть, после чего дообучиваем ее на целевых данных и целевой задаче. Такой процесс будет работать, если признаки для переноса являются *общими,* а не *специфическими*, т.е. подходят для решения как базовой, так и целевой задачи.

Если целевой набор данных значительно меньше базового, перенос обучения может быть мощным инструментом для обучения большой целевой сети без эффекта переобучения. Данная техника позволяет добиваться действительно впечатляющих результатов [3].