

КИЛЯЧКОВ Анатолий Анатольевич — кандидат технических наук, старший научный сотрудник; эксперт Центра исследования проблем безопасности РАН (119334, Россия, г. Москва, ул. Гарибальди, 21-б; AAKil@mail.ru)

ЧАЛДАЕВА Лариса Алексеевна — доктор экономических наук, профессор; профессор кафедры экономики организации Финансового университета при Правительстве РФ (125993 Россия, г. Москва, ГСП-3, Ленинградский пр-кт, 49; Chaldaeva45@mail.ru)

КОРОЛЕВ Денис Андреевич — кандидат юридических наук; партнер компании «Эрнст энд Янг» (denis.a.korolev@ru.ey.com)

БАЙЕР Андрей Викторович — партнер компании «Эрнст энд Янг» (andrew.bayer@ru.ey.com)

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ВЫЯВЛЕНИЯ ПРИЗНАКОВ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ В ХОДЕ ВЫБОРОВ

Аннотация. В современных условиях одним из путей достижения Россией лидирующих позиций является использование более качественных управленческих решений. Для этого необходимо применять новые методы и цифровые технологии управления, в т. ч. с использованием искусственного интеллекта. Одной из важных проблем, которая может быть решена подобным образом, является выявление признаков мошеннических действий в процессе выборов. Возможность использования ИИ для выявления признаков мошеннических действий в ходе выборов обусловлена тем, что в России процедура выборов на избирательных участках контролируется путем видеонаблюдения. В статье обсуждается, каким образом можно использовать получаемую в ходе выборов информацию для решения поставленной задачи. Автор отмечает, что искусственный интеллект должен выполнять функцию рекомендательной системы, оставляя за человеком обязанность принятия окончательного решения.

Ключевые слова: искусственный интеллект, нейронные сети, выборы, видеонаблюдение, выявление фактов мошеннических действий

В октябре 2017 г. на заседании Международного дискуссионного клуба «Валдай» президент России В.В. Путин сказал: «Мир вступил в эпоху стремительных перемен... Обостряется конкуренция за место в мировой иерархии. При этом многие прежние рецепты глобального управления, преодоления конфликтов и естественных противоречий уже не годятся, часто не срабатывают, а новые еще пока не выработаны»¹. В сложившейся ситуации для России возникает возможность вырваться в мировые лидеры [Караганов 2021], и нам следует воспользоваться этим шансом, хотя ресурсов для этого не так много.

В существующих условиях одним из способов добиться лидирующих позиций в мире является использование более качественных управленческих решений. Для этого необходимо применять новые методы и цифровые технологии управления, включая искусственный интеллект и анализ больших данных².

Справедливости ради следует отметить, что термин «искусственный интеллект» (ИИ) — далеко не самый удачный, т.к. вводит в заблуждение читателей, которые начинают «очеловечивать» этот термин. Правильнее использовать

¹ Материалы заседания Международного дискуссионного клуба «Валдай». — *Официальный сайт Президента России*. 19.10.2017. Доступ: <http://www.kremlin.ru/events/president/news/55882> (проверено 22.08.2021).

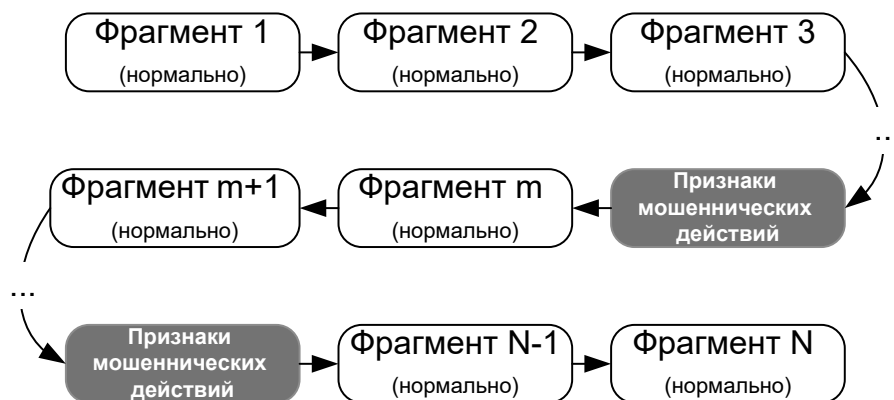
² Материалы заседания Совета по стратегическому развитию и национальным проектам. — *Официальный сайт Президента России*. 19.07.2021. Доступ: <http://kremlin.ru/events/president/news/66217> (проверено 23.08.2021).

более нейтральный термин «нейронные сети» (НС), функциональное наполнение которого то же, что и у термина «искусственный интеллект», но он не имеет такого антропоморфного оттенка. НС – это программа, которая позволяет найти оптимальное (по выбранному критерию) решение задачи, зависящей от огромного числа параметров в многомерном пространстве.

Для того чтобы задача могла быть решена с использованием нейронных сетей, она должна удовлетворять следующим требованиям: 1) задача не может быть решена алгоритмическим способом или перебором различных вариантов; 2) она уже выполняется человеком; 3) существует большая база данных, содержащих информацию о решаемой задаче с указанием правильных и неправильных решений (размеченная информация).

Одной из важных проблем, которая полностью удовлетворяет поставленным требованиям, является задача выявления признаков мошеннических действий (девиантного поведения) в процессе проведения выборов. Это следует из того, что 1) проведение выборов на избирательных участках контролируется путем видеонаблюдения; 2) процесс фиксируется в формате видеофайлов; 3) в ходе выборов и после них видеозаписи проверяются контролерами, которые выявляют признаки совершения вбросов и других мошеннических действий. Таким образом, данная задача является интеллектуальной, решаемой людьми и задокументированной в видеоматериалах. При этом, т.к. видеоконтроль за выборами осуществляется не первый год, объем данных должен быть достаточно большим.

Обсудим, каким образом можно использовать имеющуюся информацию для решения задачи выявления девиантного поведения в процессе проведения выборов с использованием нейронных сетей. Видеозаписи с избирательных участков можно рассматривать как потоковое видео, представляющее собой последовательный временной информационный ряд. Видео может быть разбито на фрагменты, содержащие информацию о происходящих событиях (см. рис. 1). Желательно, чтобы длительность фрагмента была достаточной, чтобы на нем было зафиксировано какое-либо логически завершенное действие, допустим, опускание бюллетеня в урну. Фрагменты могут содержать как нормальные события, так и девиантное поведение, содержащее признаки противоправных действий. Эти данные можно использовать для обучения НС.



Источник: Составлено авторами.

Рисунок 1. Представление видеозаписей с избирательных участков, разбитых на фрагменты, которые содержат информацию о происходящих событиях

Оценим, будет ли объем видеoinформации достаточен для обучения нейронной сети. На выборах в сентябре 2018 г. видеонаблюдение применялось на более чем 14,5 тыс. избирательных участках¹, где голосуют примерно 80% избирателей России². В 2021 г. выборы будут проходить в течение трех дней, причем избирательные участки будут работать каждый день по 12 ч. Таким образом, объем видеозаписи должен составить более 500 тыс. ч. Принимая во внимание, что на выборах 2021 г. объем видеотрансляции с избирательных участков планируется увеличить более чем в 15 раз по сравнению с предыдущими³, объем видеозаписей может составить 7,5 млн ч. Если выбрать длительность фрагмента видеoinформации равным 3 мин., то получаем 150 млн обучающих фрагментов. Таким образом, размер обучающей базы данных более чем достаточен.

Для того чтобы использовать полученную информацию для обучения нейронной сети, ее необходимо разметить, т.е. указать, какие видеофрагменты содержат признаки мошеннических действий, а какие – нет. Выявление и фиксация признаков правонарушений проводятся в процессе обработки результатов выборов. Необходимо только, чтобы эта фиксация осуществлялась в соответствии с согласованным протоколом информационного обмена, который позволяет в дальнейшем использовать эту базу данных для обучения НС.

Остается открытым вопрос о сбалансированности обучающей базы данных. Как показывает история выборов в Российской Федерации, на большинстве избирательных участков они проходят без правонарушений. Таким образом, объем видеоданных без правонарушений значительно больше, чем с правонарушениями. Это приводит к несбалансированности обучающей базы. Принимая во внимание огромный объем видеозаписей (7,5 млн ч), его можно сократить за счет фрагментов, не содержащих факты правонарушений, приведя их число в соответствие с числом фрагментов, содержащих признаки мошеннических действий. Однако здесь есть опасность, что в результате можно получить маленькую базу. Будет ли эта опасность реализована или нет, можно проверить только экспериментально, работая с реальной информацией и прототипом нейронной сети.

После того, как будет сформирована обучающая база данных и разработана финальная архитектура нейронной сети, необходимо провести ее обучение. Обученную нейронную сеть можно использовать в дальнейшем для выявления признаков мошеннических действий при проведении очередных выборов.

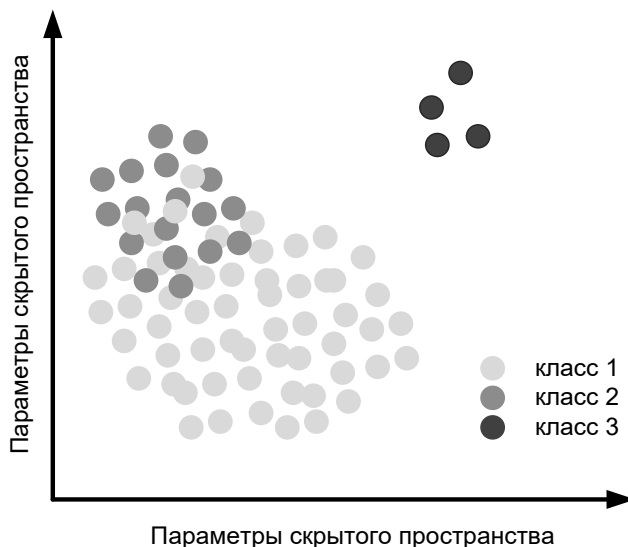
Возможен другой способ использования имеющейся базы данных для обучения нейронной сети, при котором сеть обучается на фрагментах, содержащих обычные для выборов действия. Затем с помощью этой обученной сети анализируется информация, получаемая в ходе проведения выборов. В процессе анализа нейронная сеть выявляет видеофрагменты, содержащие девиантное поведение, т.к. они отличаются от фрагментов, на которых сеть была обучена ранее. Такие нейронные сети называются автокодировщиками. Заметим, что видеофрагменты в процессе обработки нейросетью могут быть разделены на

¹ Портал видеотрансляций с избирательных участков начинает работу. – *Официальный сайт Центральной избирательной комиссии РФ*. 08.09.2018. Доступ: <http://www.cikrf.ru/news/cec/40691/> (проверено 19.08.2021).

² Элла Памфилова рассказала ТАСС о развитии избирательной системы в России. – *Официальный сайт Центральной избирательной комиссии РФ*. 11.01.2021. Доступ: <http://www.cikrf.ru/news/cec/48675/> (проверено 20.08.2021).

³ Состоялось 28-е заседание ЦИК России. – *Официальный сайт Центральной избирательной комиссии РФ*. 22.07.2021. Доступ: <http://www.cikrf.ru/news/cec/49842/> (проверено 19.08.2021).

три класса (см. рис. 2): 1) когда не происходят активные действия; 2) когда происходят обычные для выборов действия и 3) когда зафиксировано девиантное поведение (вброс, подделка бюллетеня и т.п.).



Источник: Составлено авторами.

Рисунок 2. Представление результатов работы автокодировщика, содержащих информацию о характере происходящих событий, в скрытом пространстве НС

Конечно, только человек может дать окончательное заключение о наличии признаков, указывающих на противоправное поведение, а суд устанавливает виновность того или иного лица. Но нейронные сети могут значительно ускорить и облегчить выявление подобных фактов, повысить эффективность работы контролеров и значительно снизить расходы Центральной избирательной комиссии на выявление противоправных действий.

Заметим, что аналогичную нейронную сеть (только обученную на других обучающих данных) можно использовать для контроля девиантного поведения выпускников при сдаче ЕГЭ.

Список литературы

Караганов С.А. 2021. О третьей холодной войне. – *Россия в глобальной политике*. № 4. Доступ: <https://globalaffairs.ru/articles/o-tretej-holodnoj-vojne/> (проверено 17.08.2021).

KILYACHKOV Anatoliy Anatol'evich, *Cand.Sci. (Techn.Sci.), Senior Scientific Researcher; Scholar of Security Problems Studies Centre of the Russian Academy of Science (21b Garibaldi St, Moscow, Russia, 119334; AAKil@mail.ru)*

CHALDAEVA Larisa Alekseevna, *Dr.Sci. (Econ.), Professor of the Chair Economics of Institution, Financial University under the Government of the Russian Federation (49 Leningradsky Ave, GSP-3, Moscow, Russia, 125993; Chaldaeva45@mail.ru)*

KOROLEV Denis Andreevich, *Cand.Sci. (Legal), partner at EY (denis.a.korolev@ru.ey.com)*

BAYER Andrey Viktorovich, *partner at EY, (andrew.bayer@ru.ey.com)*

USING AI TO DETECT INDICATORS OF ELECTORAL FRAUD

Abstract. *In the modern world, one of the ways for Russia to achieve a leading position is to have better quality of management decisions. This requires new methods and digital technologies of management, including the use of artificial intelligence or (in more correct and neutral terms) neural networks. One can solve the task using neural networks if it requires an intellectual effort and is already performed by a person. In addition, there must be a large database with information on the problem. Identification of fraud during the elections is one of the important problems that can be solved using neural networks. Use of neural networks is possible as the election process at polling stations is monitored by video surveillance, where the video recordings are checked by controllers. We estimated that the 2021 elections would record 7.5 million hours, which is sufficient to develop and train the neural networks. The article discusses how the information recorded during the elections can help to fraud identification. The author notes that neural networks should be used in the recommendations capacity, leaving it to the individuals to make the final decision.*

Keywords: *artificial intelligence, neural networks, elections, identification of facts of fraudulent activities, video surveillance*