

© **Дамир Маратович Апкаев**
старший преподаватель кафедры
уголовного права и криминологии
юридического факультета
ВЮИ ФСИН России,
г. Владимир
mail: damirrrhan@mail.ru
тел: 8(906)611-39-19

Apkaev D. M.
Lecturer of the criminal Law Department
and Criminology of the faculty of law of
THE VUI FSIN of

© **Александр Сергеевич Логозинский,**
курсант ФГКОУ ВО
«Нижегородская академия МВД
России»
E-mail: logozinski.sasha@icloud.com

Logozinsky A. S.,
cadet of the Nizhny Novgorod
Academy of the Ministry of Internal
Affairs of Russia

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЦЕЛЯХ БОРЬБЫ С ПРЕСТУПНОСТЬЮ

Using artificial intelligence to fightwith crime

Аннотация: в настоящей статье рассматриваются возможности использования искусственного интеллекта и нейронных сетей в борьбе с преступностью.

Abstract: This article discusses the possibilities of using artificial intelligence and neural networks in the fight against recidivism.

Ключевые слова: искусственный интеллект, нейронные сети, борьба с коррупцией, киберпреступность, кибермошенники.

Keywords: artificial intelligence, neural networks, fight against corruption, cybercrime, cyber fraudsters.

Развитие технологий открывает для преступников новые возможности. По мере развития преступлений должны развиваться и методы борьбы с ней, иными словами, «современные проблемы требуют современных решений». Следовательно, в борьбе с преступностью необходимо быть гибкими и изобретательными [5, с. 11]. В автоматизированном будущем искусственный интеллект в сочетании с наукой о данных и аналитикой даст возможность для борьбы с преступлениями – как для предотвращения, так и для расследования.

Люди – изобретательные существа, но трудолюбие – это качество, которого нам не хватает. Многократно выполнять одну и ту же задачу и обеспечивать качество – это то, в чем мы не очень хороши. Человек также связан эмоциями, которые могут влиять на принятие решения в зависимости от разных ситуаций.

Необходимо рассмотреть основные плюсы, которые может дать искусственный интеллект (далее – ИИ). Такие компании, как Yahoo!, используют

ИИ для подготовки простых документов о спортивных событиях и выборах. ИИ получит доступ к интернету, найдет необходимую и актуальную информацию и превратит ее в отчет. В области электронной коммерции ИИ используется для персонализации веб-сайтов для клиентов – показывая им, чего они хотят, и рекомендуя им продукты. Илон Маск недавно написал в Твиттере, что люди скоро вызовут свои машины, а не пойдут к своей машине. ИИ используется для анализа фондового рынка и составления прогнозов, а не их человеческие аналоги.

Киберпреступность не стоит на месте, и с момента принятия конвенции о преступности в сфере компьютерной информации она серьезно шагнула вперед, появилось множество новых видов преступлений, совершаемых с использованием компьютерных технологий: фишинг, фарминг, кибертерроризм, пиратство. Стали вырабатываться новые схемы совершения преступлений, которые значительно усложнили возможность их обнаружения, например, наркотики стали сбывать через даркнет. Финансовые компании стали внедрять в свою деятельность ИИ и нейронные сети для сокрытия своих киберследов преступлений и запутывания органов следствия. С каждым днем количество совершенных преступлений с использованием электронных средств увеличивается экспоненциально.

Борьба с киберпреступностью усложняется рядом факторов:

- 1) киберпреступники – это высококвалифицированные специалисты в области программирования; соответственно вычислить такую личность гораздо сложнее;
- 2) нехватка кадров, способных оказать противодействие кибермошенникам;
- 3) отсутствие возможности провести квалифицированную экспертизу, что приводит к трудностям доказывания факта совершения преступления;
- 4) трудно осуществлять контроль за киберпреступлениями, поскольку они постоянно обновляются и совершенствуются;
- 5) наука (киберкриминология), занимающаяся изучением киберпреступлений, находится на стадии формирования.

Необходимость охраны прав и свобод граждан неминуемо влечет за собой совершенствование средств и способов борьбы с преступностью, а также внедрение новых технологий для возможности оказывания противодействия киберпреступности.

В настоящее время пассивный режим работы электронных баз МВД России и других ведомствах устарел. Огромный массив информации вынуждает сотрудников правоохранительных органов тратить большое количество времени при работе с ним. Отсюда напрашивается необходимость усовершенствования баз путем внедрения ИИ в алгоритм их работы [4, с. 70].

Необходимо создать такую систему, которая на основе имеющихся в ней данных анализировала бы ситуацию, получаемую в онлайн-режиме через камеры видеонаблюдения, а также обобщало бы ее.

Такая система позволит сэкономить как временные, так и финансовые затраты на розыск лиц, совершивших преступления. Позволит пресечь

преступные посягательства еще на стадии покушения. Этого можно достигнуть путем внедрения нейронных сетей.

Нейронные сети – это то, что позволяет находить некоторые зависимости в свойствах данных. Они способны самосовершенствоваться и учиться, что делает их похожими на человеческий мозг. Мы можем встретиться с нейросетями, например, попросив голосового помощника включить нам что-то (музыку, фильмы) или ответить на какой-либо вопрос.

Нейроны помогают банкам принять решение по поводу выдачи кредита, решают, какую рекламу нам показать на основе предыдущих поисковых запросов в интернете. ИИ позволяет сократить большинство сотрудников техподдержки при решении стандартных запросов пользователей.

В связи с этим можно использовать нейросети при:

- 1) анализе поступивших заявлений и выдвижении простых следственных версий, определить направления их проверки;
- 2) выстраивании следовой картины, полагаясь на данные предыдущих уголовных дел;
- 3) предложении вариантов действий следователю в условиях информационной недостаточности;
- 4) поиске компьютерных файлов, сокрытых стеганографией или ADS, расшифровании их, подборке к ним пароля;
- 5) повышении эффективности при выявлении подлогов в документах путем автоматизации их признаков.

В связи с этим необходимо обеспечить равные технические возможности для всех подразделений правоохранительных органов и объединить базы данных, а также оперативно-справочные учеты. За основу целесообразнее брать базу данных ГИАЦ МВД, так как она содержит технические возможности для реализации.

Так, в ФБР ИИ применяется для обработки аудио-, видеофайлов, при банковских транзакциях. Ведутся и редактируются биометрические базы данных. Выявляются случаи мошенничества и взлома платежных систем POLPAY. Обнаруживаются и удаляются вредоносные программы в платежных системах. Изучается индивидуальный почерк хакера, обнаруживаются сетевые атаки и их локализация с помощью ИИ Mayhem [2, с. 147].

Применение нейронных сетей может выявить проявление коррупции. Ученые заявили о том, что можно спрогнозировать преступления коррупционной направленности на период до трех лет. Для этого необходимо ИИ научить делать расчеты на основании макроэкономических и политических показателей в зависимости от характеристик конкретного региона [4, с. 30].

Также при использовании ИИ для противодействия коррупции решается ряд задач:

- 1) предупреждение коррупционных преступлений. Спрогнозированные ИИ преступления коррупционной направленности повысят эффективность выявления коррупционеров и возможность пресечения их деятельности, что будет побуждать чиновников отказаться от коррупционной деятельности;

2) повысится уровень доверия населения к антикоррупционным мерам, применяемыми органами государственной власти. Эффективная работа ИИ в области противодействия коррупции будет способствовать повышению уровня доверия граждан к власти;

3) автоматизация системы борьбы с коррупцией позволит обеспечить оперативный сбор интересующей информации и применение мер по ее предотвращению;

4) создастся такой механизм противодействия коррупции, который будет функционировать без человека.

Примером эффективности использования ИИ может служить система Zero Trust, она позволила выявить тысячи коррупционеров и собрала доказательственную базу. Работа этой системы была основана на сопоставлении баз данных разных уровней с доходами и расходами государственных служащих. Это позволило выявить распространённые коррупционные правонарушения, например, махинации при производстве тендеров, необоснованную передачу прав собственности на ценное имущество, злоупотребления в сфере земельных отношений и др. Конечно, система не могла однозначно указывать на совершение конкретного коррупционного преступления или правонарушения, но она анализировала огромный массив информации, экономя время и позволяя оператору сосредоточиться на более важных моментах.

Также Великобритания использует информационные технологии для борьбы с преступностью. Здесь впервые был использован робот системы ИИ ACE, разработанный компанией Ravn. Он появился в органе прокуратуры Serious Fraud Office (далее – SFO). SFO специализируются на сложных в раскрытии случаях мошенничества, коррупции, взяточничества. Принцип работы ACE совместим с принципом работы следователя. Также робот способен пополнять собственную базу данных и обучаться идентификации необходимых документов и получению из них информации, имеющей значение для расследования преступления.

ИИ в сфере борьбы с преступностью станет огромным бонусом. Преступления совершаются людьми, и человек как логическое существо следует шаблону – какими бы случайными ни старались быть. Преимущество ИИ заключается в том, что он может обнаружить закономерности в поведении человека, он сможет предсказать, как человек будет действовать, и в этом сила ИИ.

Так, в 70-х годах прошлого века в США сотрудники полиции занимались поиском серийного убийцы Зодиака. По официальным данным, им совершено 5 убийств, но, как утверждается, количество жертв достигает 37. Он написал в полицию 4 шифра для выяснения своей личности, которые невозможно разгадать для большинства экспертов. Только один из 4 шифров был раскрыт. В современное время компьютер под названием CARMEL был настроен так, чтобы думать, как убийца Зодиак. Таким образом, CARMEL проходит через интернет, чтобы получить миллиарды ключей, чтобы попытаться раскрыть шифр Зодиака. Это то, что человек не может сделать сам.

ИИ имеет гораздо больше возможностей, таких как обнаружение выстрелов, улучшение анализа видеозаписей с камер видеонаблюдения, прогнозирование будущих мест преступности и прогнозирование того, кто будет совершать преступления в будущем.

Благодаря ИИ прошлые преступления могут предсказать возможность будущего преступления, а также где и когда оно может произойти. Этого можно достичь, проанализировав прошлые преступления, найдя сходство, а затем придумав прогнозный анализ. Их алгоритм может помочь полиции сохранять бдительность в прогнозируемых областях [1, с. 4].

ИИ может помочь нам бороться с преступностью совершенно по-новому. По мере того, как использование искусственного интеллекта увеличивается, будет уменьшаться количество преступлений, поскольку прогнозный анализ предотвратит преступность, и когда он начнет доказывать свою ценность, начнет сдерживать потенциальных преступников, и именно так можно бороться с преступностью.

Таким образом, искусственный интеллект, работа которого основана на нейронных сетях и алгоритмах самообучения, может стать эффективным помощником в деятельности правоохранительных органов по борьбе с преступностью.

Список литературы

1. Арыстанбеков М. А. Внедрение искусственного интеллекта в сферу борьбы с преступностью / М. А. Арыстанбеков // Актуальные проблемы современности. – 2021. – № 4(34). – С. 1-10.
2. Слесарева А. М., Смирнов В. М. Искусственный интеллект в деятельности сотрудников ОВД: система распознавания лиц / А. М. Слесарева, В. М. Смирнов // Тенденции развития науки и образования. – 2021. – № 79-1. – С. 147-149.
3. Попова Н. Ф. Применение технологий искусственного интеллекта в правоохранительной деятельности / Н. Ф. Попова // Административное право и процесс. – 2021. – № 3. – С. 29-32.
4. Мишин С. А., Мишин А. В. Возможные направления применения искусственного интеллекта в деятельности органов внутренних дел Российской Федерации / С. А. Мишин, А. В. Мишин // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2021. – № 7-3. – С. 68-74.
5. Ткачук Т. А., Михайлов А. Е., Цапанов Р. Е. Социальная инженерия как способ манипуляции людьми с целью получения информации или доступа к ней: обзор проблемы / Т. А. Ткачук, А. Е. Михайлов, Р. Е. Цапанов // Вестник Владимирского юридического института. – 2021. – № 4(61). – С. 110-113.