УДК 343.98

И. А. Кузьмин

ИСКУССТВЕННЫЕ НЕЙРОННЫЕ СЕТИ: ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. В настоящей статье рассмотрены основные принципы работы искусственных нейронных сетей, международный опыт их использования для противодействия преступности. Предлагаются изменения организации информационного обеспечения правоохранительных органов Российской Федерации путём слияния ведущихся в настоящее время баз данных. Предлагается принципиальное изменение действующей системы статистической отчётности.

Ключевые слова: информационное обеспечение, информационно-коммуникационные технологии, нейронные сети, искусственный интеллект, компьютерные преступления, информационные преступления, уголовная статистика.

I. A. Kuzmin

ARTIFICIAL NEURAL NETWORKS: FUTURE OF USE IN LAW ENFORCEMENT

Annotation. This article considers the basic principles of the operation of artificial neural networks, the international experience of their use in crime-fighting. Adjustments in the procedure for providing with information of law enforcement agencies of Russia by merging of modern databases are proposed. A fundamental change in the current system of statistical reporting is proposed.

Keywords: information support, information and communication technologies, neural networks, Artificial Intelligence, computer crimes, information crimes, criminal statistics.

Общий объём информации, который может сохраняться всеми мировыми техническими средствами, удваивался примерно каждые 40 месяцев на протяжении 80-х гг. XX в., а с 2012 г. и по настоящее время ежедневно генерируется 2,5 экзабайтов ($2{,}5\times10^{18}$) информации [1, с. 94]. Активно развивающиеся процессы информатизации объединяют пользователей информационных ресурсов, отдалённые базы данных, информационные массивы. Значительные объёмы информации передаются посредством информационно-телекоммуникационной сети «Интернет». Так, к середине марта 2016 г. в Интернете находилось 4,66 млрд страниц, и это значение с каждым днём увеличивается [2].

Информация представляет собой огромную ценность. Данный факт в сочетании с развитием технологий, обеспечивающих передачу и обработку информации, предопределил развитие широкого спектра преступлений, связанных с незаконным доступом к информации и её использованием. К ним можно отнести создание и распространение вредоносных компьютерных программ; организацию DDOS-атак; хищения денежных средств кредитных

и иных организаций, а также их клиентов; мошенничества и многое другое (далее — информационная преступность). В связи с этим поиск, анализ и использование информации, хранящейся в базах данных и информационных массивах, а также распространяемой в сети «Интернет», становится одной из ключевых задач государства для организации противодействия информационной преступности.

Объём генерируемой информации таков, что попытки анализа и изучения информации даже в относительно небольшом сегменте сети «Интернет», например, в национальном домене верхнего уровня для России «.ru», силами отдельных людей или подразделений правоохранительных органов существенно затруднены. Кроме того, обнаружение информации, связанной с преступной или иной противоправной деятельностью в сети «Интернет», нередко невозможно без дополнительной проверки обнаруженных результатов или обращения к помощи специалистов. Например, в случаях обнаружения экстремистских текстов на национальном языке или при работе с зашифрованными данными.

В связи с этим в ряде стран для организации противодействия информационной преступности предпринимаются активные меры на государственном уровне. Любопытен пример реализации проекта «Золотой щит» в Китайской народной республике (неофициальное название — «Великий китайский файрвол»). Для реализации проекта потребовались сотни миллионов долларов, а в разработке принимали участие многие международные корпорации [3].

Представители Министерства общественной безопасности Китая объяснили внедрение проекта «Золотой щит» «необходимостью использования передовых информационно-телекоммуникационных технологий для усиления борьбы с преступностью со стороны спецслужб и повышения оперативности их реакции, наряду с увеличением продуктивности и эффективности работы полиции» [3].

На данный момент «Золотой щит» реализует множество функций, в их числе блокировка доступа жителей КНР к внешним ресурсам сети «Интернет» (Twitter, Facebook, Google, YouTube и др.), а также блокировка доступа к ресурсам, имеющим в соответствии с законодательством КНР запрещённый контент (сайты, содержащие темы, связанные с критикой руководства КНР или коммунистической партии Китая, сайты порнографического содержания и т. д.).

«Золотой щит» осуществляет фильтрацию DNS-запросов и их переадресацию, блокировку интернет-адресов (URL) и IP-адресов, блокировку соединений, осуществляемых через VPN. По некоторым оценкам, функционирование проекта в настоящее время обеспечивает более 30 тыс. сотрудников [4].

Анализ информации, доступной из открытых источников, показывает, что приоритетом проекта «Золотой шит» является, прежде всего, блокирование нежелательного контента, т. е. в основном профилактика отдельных видов информационной преступности. В этой связи интерес представляет опыт и других стран, где реализуются проекты и используются программно-инженерные решения в области связи и информации, направленные на решение других задач правоохранительной деятельности. В частности, особое внимание

привлекает опыт развитых стран по реализации мер, направленных на выявление и раскрытие информационных и иных преступлений.

К числу стран, обладающих значительным опытом по противодействию информационным преступлениям, безусловно, относится США. На территории США действует National Crime Information Center (NCIC) [5]. В соответствии с информацией, размещённой на официальном сайте ФБР, NCIC — это электронный центр информации о преступности, который может быть использован практически всеми правоохранительными органами на всей территории США круглосуточно. Это помогает задерживать преступников, находить пропавших без вести и похищенную собственность, а также идентифицировать террористов.

База данных NCIC в настоящее время содержит сведения в 21 сегменте (файле), к основным из которых можно отнести сегменты (файлы), содержащие информацию о похищенном имуществе, оружии, номерных знаках, деталях, ценных бумагах, транспортных средствах и т. д. Также NCIC структурирует информацию о лицах, причастных к совершению преступлений против половой свободы, разыскиваемых преступниках иностранных государств, нарушителях иммиграционного законодательства, без вести пропавших, неопознанных лицах, различных категориях защищаемых лиц, террористах (известных и подозреваемых), а также иных категориях лиц, представляющих интерес. Запросы к NCIC могут осуществляться как со стационарных компьютеров, так и с мобильных устройств. Ответы на запросы поступают немедленно. NCIC устанавливает ряд мер безопасности для обеспечения конфиденциальности. Информация, проходящая через сеть, шифруется для предотвращения несанкционированного доступа. Каждый пользователь системы аутентифицируется для обеспечения надлежащего уровня доступа для каждой транзакции. NCIC периодически проверяет содержащуюся в ней информацию.

Однако и такая система уже не соответствует тем требованиям, которые выдвигает к правоохранительным органам стремительно меняющийся мир.

В. С. Овчинский отмечает, что ФБР США планирует сооружение и оснащение Центра данных и вычислений в рамках проекта N4G, который будет иметь в 50 раз большую ёмкость и скорость обработки данных, чем NCIC [6, с. 69]. Но главное в проекте N4G не объёмы серверов и быстродействие. Наиболее значимым, на наш взгляд, в проекте является применение искусственного интеллекта (далее — ИИ) на основе искусственных нейронных сетей (далее — ИНС).

ИНС — это программное или аппаратное воплощение математической модели, построенной по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма. ИНС представляет собой систему соединённых и взаимодействующих между собой простых процессоров (искусственных нейронов). Соединённые в большую сеть с управляемым взаимодействием, такие по отдельности простые процессоры вместе способны выполнять сложные задачи. Главным отличительным свойством ИНС является то, что они не программируются в привычном смысле этого слова, они обучаются. Возможность обучения — одно из главных преимуществ ИНС перед традиционными алгоритмами. Технически обучение заключается в нахождении коэффициентов связей между искусственными нейронами. В процессе обучения ИНС способна выявлять

сложные зависимости между входными данными и выходными, а также выполнять обобщение. Это значит, что в случае успешного обучения сеть сможет дать верный результат на основании данных, которые отсутствовали в обучающей выборке, а также неполных или частично искажённых данных [7].

В качестве яркого примера эффективности ИНС можно привести «нашумевший» в шахматных кругах матч ИНС AlphaZero с компьютерной программой Stockfish, состоявшийся в 2017 г. В матче было сыграно 100 партий, из которых 28 побед одержала AlphaZero и 72 партии окончились вничью. Примечательно, что AlphaZero никто не программировал, т. е. не обучал играть шахматам. Перед матчем AlphaZero 4 часа самостоятельно изучала игру в шахматы, на основе одних только введённых в неё правил игры. Этого оказалось достаточно для убедительной победы над лучшей шахматной программой мира (Stockfish — победитель чемпионата Chess.com среди компьютерных программ 2017 г.), на развитие которой у 136 программистов ушло почти 10 лет [8].

ИИ на основе ИНС уже сейчас используется для распознавания лиц по видеоизображениям, для распознавания вербальной информации и текстовой, а также решения множества иных нелинейных задач.

Таким образом, ИИ на основе ИНС — это мощное средство, которое можно и нужно использовать по множеству различных направлений.

Понимая это, информационные подразделения ФБР совместно с лабораторией искусственного интеллекта корпорации Google выработали инженерное определение искусственного интеллекта, которое будет положено в разработку концепции архитектуры и перечня программных решений для проекта N4G [6].

Очевидно, что ИИ на основе ИНС может существенно повысить эффективность анализа и систематизации генерируемой информации как в сети «Интернет», так и в базах данных и массивах информации правоохранительных органов. Тем более с учётом того, что до 95 % генерируемой информации состоит из неструктурированных данных и лишь около 5 % составляют различные базы данных, т. е. тем или иным образом структурированная информация [9].

В связи с этим специалистами ФБР при реализации проекта N4G выделяются следующие основные направления для использования ИИ:

1. Использование для обработки текстовых, аудио-, видеофайлов, информации о банковских транзакциях, данных о местонахождении физических лиц в аналитических центрах ФБР и полиции.
2. Ведение баз данных, в том числе биометрических и их редактирование.
3. Использование ИИ для экономии (за счёт сокращения сотрудников, осуществляющих в настоящее время функции, указанные в п.п. 1 и 2).
4. Обнаружение фактов мошенничества и взлома платёжных систем посредством ИИ POLPAY, разрабатываемого ФБР совместно с платёжными системами Wise и Stripe.
5. Обнаружение и удаление вредоносного программного обеспечения в действующих на территории США платёжных системах.
6. Распознавание индивидуального почерка хакеров и хакерских группировок, обнаружение сетевых атак и установление их локализации с

помощью ИИ Mayhem, разрабатываемого с 2017 г. ФБР совместно с компанией ForAllSecure и университетом штата Пенсильвания.

Безусловно, возможности ИИ не стали тайной и для преступного мира. Специалисты ФБР считают, что преступными группировками ИИ может использоваться для следующих основных задач.

1. Для операций на финансовом рынке путём проникновения в программное обеспечение торговых платформ.
2. Для хищения денежных средств со счетов кредитных организаций путём взлома платёжных протоколов.
3. Для преодоления защиты систем корпоративно-информационной безопасности.
4. Для хищений объектов интеллектуальной собственности, в том числе программного обеспечения.
5. Для совершения убийств, замаскированных под технические инциденты.
6. Для разведывательной деятельности против полиции и ФБР.

Безусловно, опыт ведущих стран мира в области борьбы с информационной и иными видами преступности необходимо использовать в работе правоохранительных органов Российской Федерации.

Сравнительный анализ информации, содержащейся в NCIC, а также информации, содержащейся в различных базах данных и информационных массивах, используемых на территории Российской Федерации, показывает следующее.

Информация о преступлениях и различных категориях лиц, представляющих интерес для органов, осуществляющих правоохранительную деятельность, в системе Министерства внутренних дел Российской Федерации содержится в Главном информационно-аналитическом центре МВД России (далее — ГИАЦ), информационных центрах на региональном уровне (далее — ИЦ), а также в экспертно-криминалистических подразделениях, на территориальном, региональном, межрегиональном и федеральном уровнях (далее — ЭКП) и в подразделениях оперативно-разыскной информации (далее — ПОРИ) [10, 11]. Часть информации, содержащейся в NCIC, в базах данных и учётах правоохранительных органов Российской Федерации отсутствует (например, информация о банковских транзакциях).

Доступ к такой информации регламентирован различными нормативными правовыми актами, при этом сроки получения информации зависят от ряда факторов: вида запроса, способа его направления, местонахождения органа, ведущего соответствующий учёт или отвечающего за редактирование базы данных, особенностей программного обеспечения, технических возможностей, а также ряда иных факторов. Данная ситуация может привести к потере оперативности при проведении следственных действий и оперативно-розыскных мероприятий (далее — ОРМ), а следовательно, и к снижению их эффективности. Объединение разрозненных баз данных и учётов правоохранительных органов, унификация их структуры, максимальная автоматизация процедуры получения содержащейся в них информации может существенно повысить эффективность и результативность предпринимаемых усилий в борьбе с преступностью. Для оперативного сотрудника территориального подразделения полиции не должно быть разницы в процедуре получения

информации из информационного центра своего региона или, например, ПОРИ иного региона. Кроме того, полагаем, что в работе с базами данных и учётами, неструктурированной информацией, в том числе размещённой в сети «Интернет», необходимо активное использование возможностей ИИ.

В связи с этим считаем, что для повышения эффективности работы правоохранительных органов Российской Федерации необходима реализация следующих мер, с учётом международного опыта борьбы с преступностью.

1. Полное слияние на базе ГИАЦ МВД России всех баз данных и учётов, поисковых систем ИЦ, ЭКП, ПОРИ.

2. Разработка на основе ИИ системы ввода полной информации о правонарушениях и преступлениях путём сканирования материалов уголовных дел, материалов об административных правонарушениях.

В данном случае предлагается после получения информации о преступлении или правонарушении и её фиксации, а также проведения следственных действий и оперативно-розыскных мероприятий, осуществлять сканирование документов, составленных по результатам этих действий и мероприятий. К числу таких документов можно отнести заявления и объяснения потерпевших, объяснения свидетелей и иных лиц, протоколы осмотра места происшествия, документы, обнаруженные в ходе обысков и выемок и другие документы. При проведении дальнейших следственных действий и ОРМ документы, подготовленные по результатам их проведения, также должны сканироваться. Информация, поступившая в результате сканирования в ГИАЦ, шифруется с помощью криптографических средств при поступлении. После поступления информации ИИ на основе ИНС осуществляется анализ поступившей информации. Выявляются признаки серийности, что крайне важно для планирования и проведения следственных действий и ОРМ по ряду категорий преступлений (убийства, кражи автомобилей, кражи с банковских карт, мошенничества с использованием информационно-коммуникационных технологий и др.), а также иные сведения, имеющие значение для дела. Существенным плюсом в такой системе является нивелирование самого понятия границ субъектов Российской Федерации, а также исключается влияние человеческих ошибок на формирование информационного массива сведений о преступлениях и правонарушениях. Безусловно, внедрение такой системы потребует как мощных программно-аппаратных средств обработки и хранения информации, так и внедрения надёжных средств шифрования информации (криптографии) и аутентификации пользователей с разграничением уровня их доступа. Дополнительно необходимо внедрение программного обеспечения, позволяющего уполномоченным пользователям осуществлять поисковые запросы по системе как по конкретным поисковым признакам (фабулы преступлений; изъятые с мест происшествий следы; имена, клички, биометрические данные подозреваемых лиц и т. д.), так и по контексту. Кроме того, при обнаружении значимой информации, система должна самостоятельно информировать об этом уполномоченных лиц. Например, после ввода следователем информации о краже, сообщать об аналогичных, ранее зарегистрированных фактах.

1. Разработка на основе ИИ системы учёта информации о лицах, подозреваемых и обвиняемых в совершении преступлений и правонарушений,

а также осуждённых путём автоматического поступления информации в электронном виде из территориальных подразделений полиции, следственного комитета, судов, учреждений ФСИН, Министерства здравоохранения и иных организаций.

В данном случае предлагается осуществлять сканирование документов о лицах, подозреваемых или обвиняемых в совершении преступлений, а также осуждённых за совершение преступлений; лицах, в отношении которых назначены принудительные меры медицинского характера; осуждённых к лишению свободы, и иных лицах (приговоры и определения суда, постановления о привлечении в качестве подозреваемого и обвиняемого, постановления об избрании меры пресечения и т. д.). Кроме того, информационный массив должен содержать сведения из различных иных официальных источников: подразделений по вопросам миграции, таможенных органов, организаций, осуществляющих перевозку пассажиров и т. д. При этом данные сведения должны направляться в ГИАЦ посредством выделенных каналов связи. Таким образом, на наш взгляд, достигается создание единого федерального пофамильного учёта лиц, совершивших или потенциально склонных к совершению противоправных деяний. Считаем целесообразным также и в этом случае внедрение программного обеспечения, позволяющего уполномоченным пользователям осуществлять поисковые запросы по системе как по конкретным поисковым признакам, так и по контексту.

2. Доступ к информации в базе данных ГИАЦ должен предоставляться как посредством стационарных компьютеров, так и мобильных устройств. Вид предоставляемой информации должен зависеть от уровня доступа конкретного пользователя. Информация ограниченного доступа, содержащаяся в ГИАЦ должна предоставляться дистанционно при реализации технических условий, предотвращающих её получение третьими лицами.

3. Анализ и систематизация информации о преступлениях и правонарушениях в ГИАЦ посредством ИНС должен дополняться анализом информации, размещённой в сети «Интернет».

Полагаем, что предлагаемые меры позволят существенно повысить качество информационного обеспечения правоохранительной деятельности, что, безусловно, положительным образом отразится и на эффективности противодействия преступности.

Список использованной литературы

1. *Качалов Д. Л., Фархадов М. П.* Исследование технологий сбора и обработки больших данных в крупномасштабных экономических системах // Изв. Волгогр. гос. тех. ун-та. — 2017. — № 15 (210). — С. 94—98.

2. Объём данных в Интернете. [Электронный ресурс]. — Режим доступа: https://www.innoros.ru/publications/analytics/16/obem-dannykh-v-internete (дата обращения: 02.03.2018).

3. Цензура в Китае: Золотой щит, или «Великий китайский файрвол». [Электронный ресурс]. — Режим доступа: https://enterchina.ru/blog/cenzura-v-kitae-zolotoy-schit-ili-velikiy-kitayskiy-fayrvol/ (дата обращения: 02.03.2018).

4. У стен есть уши. [Электронный ресурс]. — Режим доступа: https://lenta.ru/articles/2017/09/18/shield_pt1/ (дата обращения: 02.03.2018).

5. NCIC. [Электронный ресурс]. — Режим доступа: https://www.fbi.gov/ services/cjis/ncic (дата обращения 02.03.2018 г.).

6. *Овчинский В. С.* Использование искусственного интеллекта в оперативно-аналитической деятельности ФБР США. Оперативно-розыскная работа. — 2017. — № 3 (225) — С. 66—74.

7. Искусственная нейронная сеть. [Электронный ресурс]. — Режим доступа https://ru.wikipedia.org/ wiki/Искусственная_нейронная_сеть (дата обращения: 02.03.2018).

8. Stockfish. [Электронный ресурс]. — Режим доступа: https://stockfishchess.org/ (дата обращения: 02.03.2018).

9. 2018 Annual Cybersecurity Report. [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/en/us/products/security/security-reports.html (дата обращения: 02.03.2018).

10. Об организации использования экспертно-криминалистических учётов органов внутренних дел Российской Федерации: приказ М-ва внутр. Дел России от 10 февр. 2006 г. № 70. Доступ из справ.-правовой системы «Гарант».

11. О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России: приказ М-ва внутр. дел России от 19 июня 2012 г. № 608. Доступ из справ.-правовой системы «Гарант».