«Академия управления и производства»

ГЛОБАЛЬНЫЕ НАУЧНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОСТИ И ПОИСК ПУТЕЙ ИХ РАЗРЕШЕНИЯ

МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Сборник научных трудов

15 марта 2019 г.

АУП – Москва

НИЦ АРТ – Санкт-Петербург

2019

ОГЛАВЛЕНИЕ

Возможности применения и перспективы искуственного интеллекта в криминальных целях

УДК 519.86: 681.5

Вепрев Сергей Борисович

Доктор технических наук

с.н.с., заведующий кафедрой информационных технологий Московской академии Следственного комитета РФ г. Москва, Россия

veprevsb@yandex.ru

Нестерович Сергей Александрович

Кандидат технических наук,

доцент кафедры информационных технологий Московской академии Следственного комитета РФ г. Москва, Россия

sirial_2005@mail.ru

В статье зафиксирован важнейший вывод, которому раньше не уделялось такое особое внимание, что любая высокая технология имеет тройное применение: гражданское, военное и криминальное.

Ключевые слова: технологии, искусственный интеллект, экономика, информация, национальная безопасность.

The possibilities of application and the prospects of artificial intelligence for criminal purposes

Veprev Sergey Borisovich

Doctor of Technical Sciences

Senior Researcher, Head of the Information Technology Department, Moscow Academy of the Investigative Committee of the Russian Federation,

Moscow, Russia

veprevsb@yandex.ru

Nesterovich Sergey Aleksandrovich

Candidate of Technical Sciences,

Associate Professor, Department of Information Technology, Moscow Academy of the Investigative Committee of the Russian Federation,

Moscow, Russia

sirial_2005@mail.ru

The article recorded the most important conclusion, which had not been given such special attention before, that any high technology has a triple use: civil, military and criminal.

Keywords: technologies, artificial intelligence, economics, information, national security.

В период 2014 - 2016 гг. многие ведущие страны мира принимали многочисленные государственные документы, касающиеся вопросов экономики, социальной политики, экологии и пр. И все они в той или иной мере соотносились с вопросами национальной безопасности отдельного государства или союза государств. Но, что характерно, в них зафиксирован важнейший вывод, которому раньше не уделялось такое особое внимание, вывод о том, что **любая высокая технология имеет тройное применение: гражданское, военное и криминальное** [4].

Следует отметить, что реализация современных информационных технологий открывают принципиально новые возможности по созданию информационных систем и инструментальных средств различного прикладного назначения, в том числе и искусственного интеллекта (ИИ). Но у каждого явления есть и обратная сторона медали. Преступные сообщества и отдельные индивидуумы также способны использовать самые современные методы обработки информации, и, порой, не менее эффективно, чем их разработчики [3].

Российский совет по международным делам 6 ноября 2018 г., провел в Москве конференцию: «Международные и социальные последствия

использования технологий ИИ»[1]. Содержание конференции было направлено на освещение трех злободневных вопросов:

- роль технологий искусственного интеллекта в трансформации международных отношений;
- влияние искусственного интеллекта на международную безопасность;
- этико-правовые и социальные последствия использования технологий искусственного интеллекта.

На конференции поднимался вопрос, об использовании ИИ преступными сообществами в своих интересах. Было отмечено, что пока еще не замечены признаки целенаправленных усилий преступных сообществ по созданию своих собственных уникальных разработок в области ИИ. В настоящее время преступники, которые работают в сферах: финансов, контрабанды, нелегальной купли-продажи интеллектуальной собственности и т. п. используют уже разработанные программные средства, и, нужно отметить, достаточно эффективно. Преступники заинтересованы, что бы их преступную работу выполнила программа с искусственным интеллектом, а они получили от ее работы прибыль и были вне поля подозрения правоохранительных органов.

Отметим, что по сути ИИ - это программно-аппаратный комплекс, обеспечивающий поддержку и/или принятие результативных решений в динамичной, неустойчивой среде в установленное время, на основе заведомо неполной, нечеткой и не имеющей полной доказательной базы информации [1]. Говоря простыми словами, ИИ обеспечивает принятие правильных решений в реально сложившейся ситуации. При этом, сами «правильные решения» зависят от многих факторов и определить их эффективность заранее невозможно.

[1] https://russiancouncil.ru/news/v-moskve-sostoyalas-konferentsiya-mezhdunarodnye-i-sotsialnye-posledstviya-ispolzovaniya-tekhnologiy/

Сейчас преступное сообщество не стремится привлекать талантливых программистов или компаний «стартапов», которые занимаются разработками информационных систем с ИИ, для разработки собственных уникальных программ. Это связанно с тем, что сейчас в интернете в свободном доступе существует достаточное количество информационных платформ с открытым доступом программного кода[2], которые позволяют создавать собственные интерпретации программных продуктов. Многие производители IT-программ, преследуя маркетинговые цели, уже выставили свои платформы с открытым кодом, доступ к которым можно осуществить по сравнительно небольшим ценам. Поэтому, у киберпреступников есть возможность создания собственных платформ ИИ.

Раньше программисты при создании собственной программ или сервисов должны были от начала до конца разработать алгоритмы, а затем, используя те или иные языки программирования, перевести их в программный код. Сегодня создавать продукты и сервисы возможно так же, как строители строят здание — из стандартных, доставленных на стройплощадку деталей. Большинство разработок ИИ с открытым исходным кодом представляют собой контейнеры. Контейнер представляет собой платформу, на основе которой с помощью технологии API могут собираться любые сторонние программы, сервисы, базы данных и т.п. Особенностью ее использования является возможность создания соответствующих приложений, выполняющих определенные функции и взаимодействующие друг с другом. При этом, составителю совсем не обязательно разбираться в принципах функционирования и взаимодействия блоков. Цель – ввод соответствующих данных и использование этих данных при взаимодействии с внешними программами.

С 2016 года в мире растет сфера AIAS — искусственный интеллект как сервис. Этот сервис построен на разработке отдельных элементов ИИ, в

[2] http://ai-news.ru/2016/10/653138.html

первую очередь хранилищ данных, алгоритмов глубокого обучения, алгоритмов нейронных сетей, а также на программах обработки естественного языка и многомерных расчетов. Естественно, что за определенную плату имеется возможность использование этими разработками как технологиями API[3]. В таких условиях установить характер использования исходной программы крайне сложно (в принципе – почти невозможно).

В начале 2000 годов в России только несколько ведущих вузов готовило студентов с первоклассной подготовкой в области исследований и практических разработок, связанных с ИИ. В то время, правоохранительные органы вполне могли держать на контроле каждого специалиста, который мог бы использовать свои навыки в области IT и ИИ, в том числе и в корыстях целях. Сейчас для людей, которые имеют начальную подготовку в области IT, практически все университеты и вузы открыли бесплатные и платные онлайн курсы по многим компонентам в области ИИ. Это открывает возможность открытого доступа для подготовки преступного сообщества к овладению и использованию ИИ. При этом, отметим, что криминальное сообщество не будет изобретать что-то новое, оно будет использовать под свои цели, все то, что есть в свободном доступе.

По мнению открытых многих печатных изданий использование технологии ИИ преступным сообществом, особенно в развитых странах, в течение ближайших лет будет возрастать. И это связанно со следующими причинами:

1. Применение ИИ для внедрения в платежные системы вредоносного кода, с целью их дискредитации и выявления их уязвимостей. Больше всего это касается тех платежных систем, которые используют типовые протоколы криптовалют типа блокчейн и имеют P2P - архитектуру. В 2016 году, из 30 платежных сервисов, которые построены на технологии

[3] http://zavtra.ru/blogs/tramp_fbr_iskusstvennij_intellekt

блокчейн в США, только 7 из них удовлетворяли требованиям компьютерной безопасности. Отметим, что многие такие платежные системы конъюнктурны и создавались ради получении сиюминутной прибыли, задачи безопасности были поставлены на второе место. Такие системы уязвимы для построения параллельных ветвей в блокчейн или блокирования выполнения транзакций. Интеллектуальные вредоносные программы могут использовать методы глубокого обучения нейронных сетей для предварительного анализа и последующего взлома и перепрограммирования платежных протоколов такого типа.

2. Киберпреступность направленная против финансовых операций крупнейших компаний, является весьма прибыльным преступным бизнесом. Только в США ежегодно компаниями оценивается убыток от такой деятельности, в среднем, от 40 до 50 млрд долл. В настоящее время ведущие финансовые компании вкладывают большие средства в разработку соответствующих компьютерных программ на платформах с ИИ. Поэтому естественно, что киберпреступникам, чтобы сохранить свою «экологическую нишу» и долю доходов, необходимо тоже создавать компьютерные программы, которые не должны им уступать. Киберпреступность, чтобы не отстать, очевидно и неизбежно будет вынуждена использовать технологии ИИ. Тем более, что для своих преступных операций они свободно могут использовать лучшие решения с открытым кодом в на базе AIAS.

3. Известно, что гораздо выгоднее купить украденную информацию: данные, схемы, технологии или коды программы и т.д., чем тратить огромные деньги на собственные аналогичные разработки. Причем еще не известно, будет ли, достигнут желаемый результат исследований от собственных разработок. Академия ФБР и фармацевтическая корпорация Sanofi произвела исследование, на примере Индии. Было установлено, что один вложенный доллар для кражи интеллектуальной собственности в фармацевтике экономит производителям от 17-20 долл. собственных разработок. Использование современных технологий только расширяет

возможности шпионажа и использование ИИ для экономического шпионажа и кражи нужной информации становится очевидным. Так, например, внутри некоторых корпоративных сетей американского high-tech и биотехнологий действуют многоцелевые и многофункциональные хакерские программные модули, которые построенные на основе самоорганизующихся нейронных сетей. Поскольку данное направление деятельности является очень доходным, то вывод очевиден: если есть спрос, то будет и предложение.

4. На закрытых конференциях правоохранительных органов отмечалось [1], что в течение последних лет оперативные работники под прикрытием и осведомители периодически сообщали, что в преступных сообществах возникают идеи различных вариантов убийств, которые умело маскируются под несчастные случаи, используя насыщенные компьютерами автомобили, медицинские комплексы, системы управления лифтами и т. п. Поэтому в России, так и в других передовых странах, можно ожидать появления принципиально новых видов преступлений, связанных с использованием технологий ИИ. Уже сейчас Следственному комитету России, МВД, ФСБ, ФСО и СВР нужно всерьез готовиться к появлению криминальных сообществ, которые будут применять высокотехнологичные устройства, использующие методы и средства ИИ. Это могут быть заказные убийства, террористические акты, диверсии, причем они могут быть ловко замаскированы под различного рода случайные инциденты.

5. Важным инструментом криминала могут также стать хакерские программы на основе технологий ИИ, направленные на внедрение в существующие автоматизированные информационные системы. Особенность заключается в следующем. Как правило, автоматизированные информационные системы либо имеют централизованную систему управления на основе единого вычислительного центра, либо территориально-распределенную, на основе нескольких вычислительных центров. Создание программ, способных самостоятельно искать возможности подключения к центральной системе управления, создает новые

еще не изученные угрозы информационной безопасности. Замаскированное злонамеренное воздействие на другую информационную систему может быть осуществлено под видом технического или программного сбоя, имитацией внештатной ситуации, модификацией системных параметров. Сейчас даже трудно представить весь спектр возможных угроз. А в результате все происшедшее будет выглядеть как несчастный случай при неблагоприятном стечении обстоятельств.

Особо надо отметить, что обозначенные угрозы национальной безопасности России связаны не только с отдельными киберпреступниками или их группировками. Вопрос стоит и об общем противостоянии стратегических интересов России и стран Запада и, прежде всего, США. Причем реализация вредоносного информационного воздействия может быть аналогичной простой преступности или маскироваться под нее. Президент США Дональд Трамп в представленном в Конгресс проекте государственного бюджета на 2020 финансовый год предложил значительно увеличить расходы на оборону, причем 9,6 млрд долларов из военного бюджета предлагается выделить на операции киберкомандования США (US Cyber Command, USCYBERCOM). Справка: в 2019 году было выделено чуть больше 700 млн долларов. Само за себя говорит это планируемое почти в 14 раз увеличение расходов.

Итак, с одной стороны, в настоящее время в спецслужбах и правоохранительных органах России явно не хватает специалистов, которые могли бы на высоком профессиональном уровне разобраться во всех тонкостях перечисленных выше вызовов. Очевидно, требуется создание специальных групп, отделов, а, может быть, и управлений, направленных на борьбу именно с киберпреступностью в сфере высоких технологий.

С другой стороны, для реализации возможностей защиты национальной безопасности России в сфере высоких технологий требуется уточнить и дополнить законодательную базу, которая в настоящее время отстает от реалий и зачастую не в состоянии обеспечить эффективное противодействие

киберпреступности. Законодательные изменения в такой сложной сфере также потребуют привлечения к работе высококлассных специалистов,

способных совокупно оценить технические, экономические, социальные и правовые аспекты и возможные последствия их законодательной реализации.

Список литературы

1. Бяхов О. Юриспруденция и искусственный интеллект: наступает эпоха беспрецедентных вызовов // Материалы закрытой экспертной дискуссии клуба «Валдай» и АО «РВК» «Юриспруденция: что ждёт право в эпоху роботов и искусственного интеллекта?». URL: http://ru.valdaiclub.com/events/posts/articles/yurisprudentsiya-i-iskusstvennyy-intellekt-nastupaet-epokha-bespretsedentnykh-vyzovov/ (дата обращения: 10.04.2018).

2. Выступление Президента РФ В.В. Путина на расширенном заседании коллегии МВД России от 28 февраля 2018 г. URL: http://kremlin.ru/events/president/transcripts/56949 (дата обращения: 10.04.2019).

3. Ларина Е.С. Овчинский В.С. Искуственный интеллект. Большие данные. («Коллекция Изборского клуба») – М,: Книжный мир, 2018. – 416 с.

4. Овчинский В.С. Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. — М. : Норма : ИНФРА_М, 2018. — 352 с.

5. Состояние преступности в Российской Федерации за январь - декабрь 2017 года. URL: https://мвд.рф/reports/item/12167987/ (дата обращения: 10.04.2019).

Bibliography

1. Byakhov O. Jurisprudence and artificial intelligence: the era of unprecedented challenges is coming // Materials of the closed expert discussion of the Valdai Club and RVC JSC “Jurisprudence: what is the right in the era of robots and artificial intelligence?” URL:

http://www.valdaiclub.com/events/posts/articles/yurisprudentsiya-i-iskusstvennyy-intellekt-nastupaet-epokha-bespretsedentnykh-vyzovov/ (appeal date: 10.04.2018).

2. Speech by the President of the Russian Federation V.V. Putin at the extended meeting of the board of the Ministry of Internal Affairs of Russia on February 28, 2018 URL: http://kremlin.ru/events/president/transcripts/56949 (appeal date: 04/10/2019).

3. Larina E.S. Ovchinsky V.S. Artificial intelligence. Big data. ("Collection of the Izborsk Club") – M.: Book World, 2018. - 416 p.

4. Ovchinsky V.S. Criminology of the digital world: textbook for magistracy / V.S. Ovchinsky. - M.: Norma: INFRA_M, 2018. - 352 p.

5. The state of crime in the Russian Federation in January - December 2017. URL: https: //mvd.rf/reports/item/12167987/ (access date: 04/10/2019).