УДК/UDC 343. 98

Криминалистически значимые особенности новейших информационных технологий

Краснова Людмила Борисовна
кандидат юридических наук, доцент
Воронежский государственный университет
г. Воронеж, Россия
e-mail: krasnova@law.vsu.ru
SPIN-код: 9512-0382

Аннотация

В статье рассмотрены криминалистически значимые особенности новейших информационных технологий: особенности создания, преобразования и использования искусственного интеллекта и его наиболее эффективного способа организации — искусственных нейронных сетей, а также программных и технических средств, обеспечивающих анонимность осуществляемых действий (это в первую очередь электронные средства общения, минующие операторов связи, и более сложные средства, такие как анонимайзеры, VPN, специальные браузеры). Большинство перечисленных информационных технологий создают и непрерывно ведут запись всех производимых с ними действий. Таким образом, электронная техника обладает способностью хранить значительный объем цифровой информации и является на данный момент самым информативным источником сведений о его владельце и его активности в цифровой среде, что создает возможность криминалистического исследования всего технологического процесса воздействия на электронную информацию.

Ключевые слова: криминалистика; расследование преступлений, совершаемых с использованием информационных технологий; информационные технологии; искусственный интеллект; анонимайзеры.

Forensic Features of the Latest Information Technologies

Krasnova Lyudmila Borisovna
Candidate of Law, assistant professor
Voronezh State University
Voronezh, Russia
e-mail: krasnova@law.vsu.ru
SPIN Code: 9512-0382

Abstract

The article discusses the forensic features of the latest information technologies: the features of the creation, transformation, and use of artificial intelligence and its most effective way of organizing (artificial neural networks), software and hardware that ensure the anonymity of the actions taken (these are primarily electronic communication tools that bypass telecom operators and more sophisticated tools such as anonymizers, VPNs, and special browsers). Most of the listed information technologies create and continuously record all actions performed with them. Thus, electronic equipment has the ability to store a significant amount of digital information and is currently the most informative source of information about its owner and their activity in the digital environment, which makes it possible to conduct a forensic investigation of the entire technological process of impact on electronic information.

Key words: forensics, investigation of crimes committed using information technology, information technology, artificial intelligence, anonymizers.

Современный этап развития общества характеризуется ростом высокотехнологичной преступности. Это связано в первую очередь с тем, что если ранее, характеризуя личность преступника, совершающего преступления с использованием информационных технологий, отмечалось, что это лица, обладающие достаточно глубокими специальными знаниями в области информационных технологий и имеющие доступ к профессиональному компьютерному оборудованию, то на данный момент ситуация существенно изменилась.

Так, например, исследования показывают, что информационно-телекоммуникационные сети для бесконтактного сбыта наркотических средств обычно используют «. . . молодые люди в возрасте 18–28 лет. Они имеют среднее техническое, высшее или незаконченное высшее образование. Многие из них имеют познания в области компьютерной техники и информационных технологий, а также активно используют их, например, при создании и обслуживании интернет-сайтов с объявлениями о продаже наркотиков. Рассматриваемые преступники ориентируются в отдельных финансовых операциях, например, особенностях движения денежных средств по счетам, вкладам в банковской системе, возможностях системы безналичного расчета через электронные системы оплаты» [1, с. 84] .

Т. е. современные информационные технологии значительно упростили процесс осуществления некоторых действий, давая возможность сложные систематически повторяющиеся действия осуществлять одному человеку, имеющему минимальные специальные знания. Причем для этого не нужно обладать какими-либо мощными электронными ресурсами. Более того, при наличии начальных знаний и навыков программирования можно организовать осуществление этих действий в автоматическом режиме.

Например, можно запрограммировать компьютер для выполнения такого действия, как отправка сообщения электронной почты в определенное время. Этот процесс называется планированием событий и не требует вообще никаких навыков программирования - это простая функция операционной системы.

В настоящее время наиболее современным видом информационных технологий является искусственный интеллект.

В законодательстве содержится следующее определение понятия: «искусственный интеллект - комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые,

как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в т. ч. в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений» [2].

Наиболее эффективным способом организации искусственного интеллектаявляются искусственные нейронные сети.

«Искусственная нейронная сеть — математическая модель, а также ее программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма.

Искусственная нейронная сеть состоит из искусственных нейронов (artificial neuron), каждый из которых представляет собой упрощенную модель биологического нейрона. Все, что делает искусственный нейрон, — это принимает сигналы со многих входов, обрабатывает их единым образом и передает результат на многие другие искусственные нейроны, т. е. делает то же самое, что и нейрон биологический. Биологические нейроны связаны между собою аксонами, места стыков называются синапсами. В синапсах происходит усиление или ослабление электрохимического сигнала. Связи между искусственными нейронами называются синаптическими, или просто синапсами. У синапса имеется один параметр — весовой коэффициент, в зависимости от его значения происходит то или иное изменение информации, когда она передается от одного нейрона к другому. Именно благодаря этому входная информация обрабатывается и превращается в результат, а обучение нейронной сети основано на экспериментальном подборе такого весового коэффициента для каждого синапса, который и приводит к получению требуемого результата» [3].

Для того чтобы нейронная сеть могла корректно решать поставленные задачи, требуется провести ее обучение на десятках миллионов наборов входных данных. Но уже разработаны различные технологии ускоренного обучения, современные видеокарты позволяют обучать нейросети в сотни раз быстрее, а недавно появились готовые, предобученные

нейросети, которые, например, могут распознавать образы. На основе таких нейросетей можно создавать приложения, не занимаясь длительным обучением [4].

В 2013 г. считалось, что создание масштабных нейронных сетей обходится очень дорого с точки зрения вычислительных ресурсов. Например, компании Google для создания сети, которая научилась всего лишь распознавать кошек в серии роликов YouTube, пришлось задействовать примерно 1000 серверов, что эквивалентно 16 тысячам процессорных ядер. Построенная сеть характеризовалась 1,7 млрд параметров, которые виртуально отражали связь между нейронами [3].

Но технологии развиваются очень быстро. В 2017 г. дочерняя компания Intel под названием Movidius выпустила на рынок устройство Neural Compute Stick. Оно имеет размеры, сопоставимые с обычной флешкой, при этом внутри находится мощная нейронная сеть с функцией глубокого машинного обучения. Стоимость этого продукта — $79 [5].

Таким образом, если раньше использование нейронных сетей при совершении преступлений было ограничено в силу трудоемкости и сложности реализации таких алгоритмов, то при современном развитии и повсеместном использовании информационных технологий это перестало быть проблемой, и создавать нейронные сети теперь могут научиться даже те, кто ранее навыков программирования не имел.

Но, с другой стороны, в основе работы любой информационной технологии, включая и искусственный интеллект, лежит программа, которую создал человек. И программа эта основана на некотором алгоритме, который и управляет поведением устройств. Это управление представляет собой процессы, состоящие из четко регламентированных правил выполнения операций, действий, этапов разной степени сложности над данными, хранящимися в электронных устройствах. При этом электронная техника создает и непрерывно ведет запись всех производимых с ней действий, сохраняя адреса веб-сайтов, которые просматривал пользователь, документы или изображения, которые были загружены или

отредактированы, использованные приложения, время и продолжительность их использования, координаты нахождения и перемещения устройства. Таким образом, электронная техника обладает способностью хранить значительный объем цифровой информации и является на данный момент самым информативным источником сведений о его владельце и его активности в цифровой среде, что создает возможность криминалистического исследования всего технологического процесса воздействия на электронную информацию.

Однако вышеизложенные принципы и тенденции развития информационных технологий создают определенные трудности для их технического исследования, т. к. обладают все более сложной и разветвленной инфраструктурой. «Одним из первых примеров использования искусственного интеллекта в широкоформатных кибератаках можно считать вирус CryptoLocker, распространявшийся при поддержке однорангового ботнета GameoverZeuS, использовавшего зашифрованные каналы связи с центрами контроля и управления. Эта вредоносная система использовала самообучающиеся алгоритмы управления, тип и характер которых в настоящее время достоверно не известен. Обезвреженный в результате операции Tovar ботнет GameoverZeuS был отрезан от центров управления, но сами центры в руки правоохранителей не попали, так что возможности проанализировать использованное для управления программное обеспечение не было. Тем не менее ряд косвенных признаков (устойчивость к контрвзлому, избегание прямых атак, адаптивное поведение, скорость принятия решений) свидетельствуют о возможном использовании нейросетевой технологии в управлении данной вредоносной компьютерной системой» [6].

Физически электронная информация может быть расположена как в памяти самого электронного устройства, так и в любой точке мира. Фактически такая информация может быть получена как из мобильных устройств (телефонов, компьютеров, ноутбуков, GPS и т. д.), так и с серверов, которые предоставляют услуги через Интернет и часто регистрируют IP-адреса и другую информацию о своих клиентах и их действиях.

Эти серверы могут быть расположены в разных странах, с разными национальными законами.

Традиционное хранение информации в виде письменных документов или на каком-либо ином материальном носителе всегда позволяло точно определить, где именно находятся те или иные сведения. А рассматривать электронные устройства как обычные предметы невозможно, т. к. традиционно юридическая наука и практика всегда исходила из того, что объект материального мира содержит лишь те сведения, что хранит в себе, в то время как электронные устройства могут предоставлять информацию, физически хранимую в иных местах. И таких мест может быть достаточно много. В связи с этим поиск интересующей следствие информации должен осуществляться как на электронных устройствах подозреваемого или обвиняемого, так и на других связанных с ними электронных устройствах, хранящих информацию, например серверах провайдеров. При этом все эти носители информации обладают способностью хранить огромный объем информации, требующий для исследования значительного времени.

Кроме того, в последнее время при совершении преступлений все больше используются не только компьютеры, методика исследования которых уже достаточно сформировалась, но и иные устройства (смартфоны, планшеты и т. д.), также имеющие свои особенности функционирования. Это, на наш взгляд, исключает формулирование конкретных рекомендаций по поиску и фиксации относимой к делу информации.

Наконец, еще одной особенностью использования информационных технологий при совершении преступлений, по нашему мнению, является появление различного вида электронных и программных средств, обеспечивающих все больший уровень анонимности осуществляемых действий. Он достигается в первую очередь за счет использования для коммуникации электронных средств общения, минующих операторов связи. К ним относятся такие программные средства, как Viber, Skype, WhatsApp. Для осуществления финансовой связи при совершении пре-

ступлений могут используются электронной платежные системы, такие как WebMoney, «Yandex-деньги», QIWI, PayPalи т. д.

Более сложным способом обеспечения анонимности является использование анонимайзеров. Главной функцией анонимайзера является маскировка IP-адреса. К таким сервисам относятся: программное обеспечение, устанавливаемое на компьютер или мобильное устройство; надстройки и дополнения веб-браузеров; удаленные прокси-серверы; онлайн-сервисы.

Самым простым и доступным является использование встроенных функций VPN, которые имеются в некоторых браузерах (например, в браузере Opera). VPN (virtual private network) представляет собой виртуальную частную сеть, пользователи которой соединяются с провайдером по закрытому каналу (тоннелю), который обеспечивает зашифрованную передачу данных. Тем самым достигается безопасность соединения, а также анонимность пользователя.

«Возникает вопрос об обеспечении сохранности сведений о пользователе на сервере провайдера. В 2013 г. интернет-ресурсом torrentfreak.com был проведен опрос, в ходе которого у VPN-провайдеров выясняли, хранят ли они журналы, позволяющие сопоставить IP-адреса. Как следует из результатов опроса, такие журналы не хранятся либо хранятся недолго, а установить по ним клиента невозможно» [7].

Еще один распространенный способ сохранения анонимности- это использование специальных браузеров. Наиболее популярным из них является TOR Browser. Он позволяет пользователю анонимно просматривать веб-страницы, скрывая фактическое имя пользователя, и защищает от любого анализа трафика.

«Работа сети построена на использовании так называемой луковой маршрутизации. Ее суть заключается в использовании системы специальных узлов, которые последовательно шифруют информацию о пользователе и маскируют действующий IP-адрес компьютера. Специальные узлы - это компьютеры и серверы нескольких тысяч пользователей, входящих в единую анонимную сеть. Как правило, соединение пользовате-

ля происходит через три случайных узла (входной, промежуточный и выходной). Каждому из указанных узлов неизвестны адреса пользователя и интересующего его ресурса одновременно (иначе говоря, известно только, откуда пришли данные и куда их необходимо отправить). Такой способ работы в сети Интернет, несмотря на низкую скорость, позволяет с достаточно большой степенью вероятности сохранить в тайне данные пользователя, обратившегося на какой-либо закрытый (заблокированный) сайт» [7].

При этом возможность контроля указанных каналов связи и платежных систем как технически, так и организационно у правоохранительных органов крайне низкая.

Другой составляющей анонимности преступной деятельности с использованием информационных технологий является то, что используемая электронная техника и программные средства, создают и непрерывно ведут журналы действий пользователя. Однако при этом идентификация истинного автора этих действий является достаточно трудной задачей. Действительно, возможно определить владельца электронного устройства и действия, на нем производимые, но сама электронная информация не содержит данных о том, кто или что непосредственнно ее произвело. Т. е. установление лица, непосредственно производившего эти действия, является не только задачей специалистов в области высоких технологий в рамках компьютерно-технической экспертизы, но и специалистов в области автороведения, дактилоскопии, речеведения и т. д.

Таким образом, значимые с точки зрения криминалистики особенности создания, преобразования и использования новейших информационных технологий, описанные выше, должны, по нашему мнению, способствовать выработке научно-обоснованных рекомендаций по расследованию высокотехнологичных преступлений.

Список литературы

1. Поляков В. В., Кондратьев М. В. Криминалистические особенности бесконтактного способа совершения наркопреступлений // Известия Алтайского государственного университета. 2015. № 2-1 (86). Т. 1. С. 83–86.

2. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 № 490 // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

3. Искусственные нейронные сети (ИНС) // Технологии IT-Enterprise. URL: https://www.it.ua/ru/knowledge-base/technology-innovation/iskusstvennye-nejronnye-seti-ins (дата обращения: 21.05.2020).

4. Хохлова Д. Бум нейросетей: Кто делает нейронные сети, зачем они нужны и сколько денег могут приносить // vc.ru. URL: https://vc.ru/future/16843-neural-networks (дата обращения: 22.05.2020).

5. Intel представила нейронную сеть размером с флешку // Hi-News.ru. URL: https://hi-news.ru/technology/intel-predstavila-nejronnuyu-set-razmerom-s-fleshku.html (дата обращения: 22.05.2020).

6. Ерахтина Е. А., Тирранен В. А. Преступления, совершаемые с использованием искусственного интеллекта: проблемы квалификации и расследования // Вестник Сибирского юридического института МВД. № 2 (35). 2019. С. 36–41.

7. Усманов Р. А. Характеристика преступной деятельности, осуществляемой в сети интернет посредством сервисов-анонимайзеров // Юридическая наука и правоохранительная практика. 2018. № 4 (46). С. 135–141.

References

1. Polyakov, V. V., Kondratev, M. V. Criminalistics Features of Non-Contact Modus Vivendi of Drug-Related Crimes // Izvestiya of Altai State University Journal. 2015. No. 2-1 (86). Vol. 1. Pp. 83–86.

2. On the Development of Artificial Intelligence in the Russian Federation: Decree of the President of the Russian Federation of October 10, 2019 No. 490 // Collection of the Legislation of the Russian Federation. 2019. No 41. Art. 5700.

3. Artificial Neural Networks (ANNs) // IT-Enterprise Technologies. URL: https://www.it.ua/en/knowledge-base/technology-innovation/iskusstvennye-nejronnye-seti-ins (access date: May 21, 2020).

4. Khokhlova, D. The Boom of Neural Networks: Who Creates Neural Networks, Why They Are Needed and How Much Money They Can Bring // vc.ru. URL: https://vc.ru/future/16843-neural-networks (access date: May 22, 2020).

5. Intel Presented a Neural Network the Size of a Flash Drive // Hi-News.ru. URL: https: //hi-news.ru/technology/intel-predstavila-nejronnuyu-set-razmerom-s-fleshku.html (accessed date: 05/22/2020).

6. Erakhtina E. A., Tirranen, V. A. Crimes Made With the Use of Artificial Intelligence: Problems of Qualification and Investigation // Vestnik of Siberian Law Institute of the MIA of Russia. No. 2 (35). 2019. Pp. 36–41.

7. Usmanov, R. A. Characteristics of Criminal Activities Carried Out on the Internet by Means of Anonymizers // Legal Science and Law Enforcement Practice. 2018. No. 4 (46). Pp. 135–141.