УДК 343.97

В. А. Тирранен
Красноярский государственный аграрный университет (Красноярск, Россия)

ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Принята к публикации 15.11.2019

Статья посвящена актуальным угрозам информационной безопасности, связанных с широким распространением компьютерных технологий. Автором рассматривается один из аспектов киберпреступности, а именно преступности с использованием искусственного интеллекта. Анализируется понятие исскуственного интелекта, предлагается определение, достаточное для эффективного правоприменения. В статье обсуждаются проблемы привлечения к уголовной ответственности за совершение таких преступлений, показаны сложности решения вопроса правосубъектности и деликтоспособности искусственного интеллекта. Автор приводит различные случаи, объясняя, почему возникают трудности в определении ответсвенного за совершение преступления лица, дает объективную оценку возможности привлечения к уголовной ответственности создателей программного обеспечения, в работе которого появились ошибки, повлекшие причинение вреда охраняемым уголовным законом правам и законным интересам.

Ключевые слова: информационная безопасность, киберпреступность, виртуальное пространство, информация, искусственный интеллект, нейросети.

DOI: 10.32324/2412-8945-2019-3-10-13

Быстрое развитие компьютерных технологий во всех направлениях науки и техники провоцирует рост организованной высокотехнологичной киберпреступности, отвоевывающей свои позиции в преступном мире. Киберпреступность в современных условиях, как отмечают специалисты, представляет одну из наиболее серьезных угроз как для информационной безопасности государства, так и для его экономического развития, являясь одной из важнейших проблем современности [9]. Особняком в современной киберпреступности стоят преступления, совершаемые с использованием искусственного интеллекта. Применение этого инструмента определяет новый уровень угрозы информационной безопасности, что требует готовности правоприменителя в борьбе с ней.

Успешность борьбы с киберпреступностью во многом определяется действенностью методики предупреждения преступности и ее соответствием характеру киберпреступности. Только наличие знаний о способах и методах преступной деятельности, об орудиях и средствах преступлений может обеспечить успешность приемов и способов противодействия преступности. Нельзя не согласиться с мнением Горазда Мешко относительно того, что киберпреступления, в отличие от «не-цифровых» преступлений, намного сложнее понять и объяснить [8]. В первую очередь это определяется тем, что киберпреступления сами по себе требуют как от преступника, так и от правоохранителя квалификации в сфере информационных технологий. К этой квалификации относится как понимание логики программирования, так и знания в области информационной безопасности и навыки практического использования или обезвреживания вредоносных программ и специализированного оборудования. Эффективное противодействие киберпреступности невозможно без соответствующих знаний и навыков как у ученого-исследователя, так и у правоприменителя.

Несмотря на то что современные цифровые технологии открывают значительные возможности для развития государств, межгосударственных объединений, а также отдельных организаций и способствуют законной деятельности, они также создают новые возможности для традиционных преступлений и почву для роста киберпреступности. Правоохранительные органы многих государств обеспокоены увеличением масштабов киберпреступности, ухудшением последствий для стабильности критически важной инфраструктуры государств и организаций, а также благополучия людей.

Для понимания преступлений, совершаемых с использованием искусственного интеллекта, необходимо определить, что понимается под искусственным интеллектом. На сегодняшний день этот термин не закреплен в нормативных актах в сфере развития цифровых технологий. В проекте Закона США об искусственном интеллекте он определяется как «любые искусственные системы, выполняющие задачи в изменяющихся и не-

ISSN 2412-8945. Развитие территорий. 2019. № 3 (17).

предсказуемых условиях без значительного надзора со стороны человека, либо способные учиться на своем опыте и повышать свою производительность» [7].

Отдельные исследователи определяют искусственный интеллект как «искусственную сложную кибернетическую компьютерно-программно-аппаратную систему (электронную, в том числе — виртуальную, электронно-механическую, биоэлектронно-механическую или гибридную) с когнитивно-функциональной архитектурой и собственными или релевантно доступными (приданными) вычислительными мощностями необходимых емкостей и быстродействия» [5].

Данные определения несколько сложны для восприятия неспециалистом и избыточно конкретизированы для эффективного правоприменения. В то же время, в узком смысле, применимом к составу преступления, искусственный интеллект предлагается определять как свойство интеллектуальных систем (включая компьютерные программы и искусственные нейронные сети) выполнять функции и решать задачи, в том числе специально не оговоренные, самообучаться и адаптировать свое поведение под воспринимаемые внешние условия, а также принимать решения исходя из этих условий и поставленных целей.

До недавнего времени использование искусственного интеллекта в преступной деятельности было ограничено в силу, с одной стороны, недостаточной автоматизации современной жизни, а с другой — объемности и ресурсоемкости самообучающихся алгоритмов. Однако с повсеместным внедрением «умной» техники в повседневную жизнь и развитием информационных технологий, в частности искусственных нейронных сетей, эти проблемы отошли в прошлое, позволив внедрить искусственный интеллект во вредоносные компьютерные программы. Эти программы (условно называемые компьютерными вирусами), так же как и биологический интеллект, подвержены влиянию такого серьезного эволюционного фактора, как конкуренция, и развиваются под ее воздействием. Даже отдельные компьютерные вирусы уже обладают некоторыми признаками искусственного интеллекта, к которым относятся адаптивное поведение (позволяющее по-разному действовать в разных условиях), самовоспроизведение с мутациями (что обеспечивает бесполезность сигнатур более старых версий), мимикрия (маскировка под легальные программы). При этом использование самообучающихся алгоритмов не должно вредить незаметности и быстродействию вредоносных программ, в противном случае они окажутся неэффективными, будут уничтожены и вытеснены конкурентами.

В последнее время появилась новая модель вирусной киберугрозы — многоуровневая вредоносная компьютерная система, сочетающая в себе элементы незаметных быстродействующих вирусов (торпед), распределенных объектов поддержки (катеров) и центра контроля и управления (флагмана), которые связаны воедино зашифрованными децентрализованными каналами связи и способны обеспечить в ходе кибератаки комбинированное использование разных типов уязвимостей (атака на отказ защитных систем, встраивание вредоносного кода, использование уязвимостей в программном обеспечении, перехват канала связи, подмена пользователя, загрузка через облачное хранилище данных и т. п.) и способов передачи информации (стандартная сеть, беспроводные сети различного диапазона, сервисные каналы связи, адаптированный доступ с сопряженных устройств, например, смартфона) [6]. Ручное управление такой системой человеком-оператором практически невозможно, особенно при большом числе одновременно атакуемых компьютерных систем, в силу невозможности принятия решений в режиме реального времени (принимаемые решения во время массированной кибератаки могут исчисляться в миллиардах операций в секунду, что несопоставимо со скоростью работы человеческого мозга). Поэтому центр контроля и управления распределенными атакующими объектами должен обладать способностями искусственного интеллекта для проведения полноценной кибератаки с использованием всех доступных возможностей.

При этом в последнее время все чаще такие вредоносные компьютерные системы (так называемые ботнеты) создаются не с использованием традиционных компьютерных устройств, таких как персональные компьютеры, планшеты и смартфоны, а с применением вычислительных мощностей «умной техники» нового поколения, входящих в так называемый интернет вещей (IoT), вычислительную сеть физических предметов, оснащенных технологиями для взаимодействия друг с другом или с внешней средой, выполняющую значительную часть действий и операций без участия человека [3]. К таким устройствам относятся умные медиацентры, автономные IP-камеры и даже холодильники. При этом опасность такого рода растет год от года — по оценкам, к сети Интернет в 2020 г. будет подключено уже не менее 24 млрд «умных» устройств [1].

Вопрос правосубъектности и деликтоспособности искусственного интеллекта на сегодняшний день не решен: появление новых интеллектуальных технологий требует конкретизации их правового положения. Некоторые ученые полагают, что искусственный интеллект должен обладать гетерогенной правосубъектностью, в зависимости от функционально-целевого назначения и возможностей [4], с введением соответствующего субъекта права — электронного лица. Другие исследователи считают, что «для приобретения искусственным интеллектом статуса субъекта права необходимо наличие у него такого качества, как воля» [2], которой он не обладает, в связи с чем наделение его правосубъектностью и деликтоспособностью все равно будет фиктивным.

Нерешенной проблемой в рассматриваемой ситуации будет привлечение к ответственности за

совершение преступления, конкретный «умысел» на которое был сформирован искусственным интеллектом: намечена цель (например, вирусная атака на конкретную компьютерную систему), найден способ (использование уязвимости в протоколе связи), сформировано средство (специально скомпилированный вирус для атаки на определенный порт), при этом сам искусственный интеллект был запущен «в действие» оператором, не являющимся разработчиком указанной системы искусственного интеллекта.

Распространенная концепция применения к искусственному интеллекту конструкции источника повышенной ответственности, к сожалению, не всегда дает внятный результат: оператор может не предвидеть возможных последствий применения устройств и программного обеспечения с признаками искусственного интеллекта, а иногда о таких последствиях не догадывается даже программист, составивший алгоритм искусственного интеллекта.

Наиболее корректным способом реализации уголовной ответственности за эти преступления может являться концепция посредственного причинения, при которой лицо совершает умышленное преступление с неконкретизированным умыслом при помощи системы с искусственным интеллектом, которая не может подлежать уголовной ответственности, но может самостоятельно определять (конкретизировать) цель посягательства и выполнять объективную сторону преступления, при этом подлежащий уголовной ответственности субъект объективную сторону преступления не выполняет.

На практике такие вопросы пока не возникают: у искусственного интеллекта отсутствует возможность совершить эксцесс исполнителя и выйти за пределы усмотрения того, кто систему разрабатывал. Свободой воли в осознанном смысле указанные системы не обладают, во всяком случае в настоящее время, и все пределы усмотрения и цели работы закладываются еще на этапах разработки программы или ее обучения.

Несколько иначе обстоят дела в ситуации, когда за создание системы отвечает одно лицо, а за запуск ее в работу — другое, при этом разработчик системы вкладывает в нее некоторые непредусмотренные возможности. Например, в дополнение к заражению компьютеров пользователей и вовлечению их в ботнет вирусная программа будет заниматься также сбором персональных данных владельца компьютера и их пересылкой разработчику вируса или иному лицу. Ботнет, арендованный оператором для проведения массированной DDOS-атаки, помимо основной цели будет стремиться получить доступ к банк-клиентам на атакуемых компьютерах и осуществить прямой вывод денежных средств на подставное лицо в оффшорной зоне. В таких случаях умысел на использование определенного преступного алгоритма у лица, запустившего его в работу, отсутствует, и вменить ему ответственность за нарушение неприкосновенности частной жизни или хищение с банковского счета не представляется возможным, поскольку именно его умыслом такое поведение вредоносной программы не охватывалось. Ответственность же в данном случае должен нести разработчик программы, как лицо, заложившее в нее такие возможности (в том числе возможность самообучения для сбора информации) и осознававшее то, что в дальнейшем она будет запущена в работу. При этом, впрочем, крайне проблемно будет выявить и доказать факт незнания оператором указанных особенностей работы программ и сетей, поскольку такие программные особенности могут быть достоверно выявлены только в изначальной или декомпилированной версии программы, доступ к которой у оператора (как и следственных органов), как правило, отсутствует.

Также необходимо отметить возможные ошибки в работе вредоносного программного обеспечения, в том числе алгоритмов искусственного интеллекта, в результате которых вопреки целевому назначению программы может быть причинен существенный вред охраняемым уголовным законом правам и законным интересам. В связи с использованием искусственного интеллекта возможны проблемы адаптации его действий к требованиям конкретных ситуаций, а также сбои в алгоритмах обучения, что тоже может повлечь за собой «незапланированные» последствия. В данном случае со всей очевидностью при квалификации необходимо будет исключить прямой умысел в отношении таких «дополнительных» последствий: в зависимости от осознания возможности их наступления и принимаемых по этому поводу мер вина может быть выражена в форме косвенного умысла (при котором виновный предвидел возможность неблагоприятного исхода, но никаких эффективных мер к его предотвращению не принял) либо в форме неосторожности по причине легкомыслия (при безуспешной попытке последствия предотвратить) или небрежности (при отсутствии предвидения вреда и наличия возможности его предвидеть). При этом предположить невиновное причинение вреда для разработчика в такой ситуации при должной его компетентности сложно: у него в любом случае есть возможность моделирования работы программы перед ее запуском, и неосмотрительность по поводу последствий будет последствием его небрежности.

Список литературы

1. *Атака* «умных» вещей [Электронный ресурс] // Nag.Ru : информ.-аналит. портал. URL: https://nag.ru/articles/article/30371/ataka-umnyih-veschey.html

2. *Васильев А. А., Шпоппер Д., Матаева М. Х.* Термин «искусственный интеллект» в российском праве: доктринальный анализ // Юрислингвистика. 2018. № 7—8. С. 39.

3. *Из чего* состоит IoT. Интернет вещей. [Электронный ресурс] // Хабр : медиапортал.

URL: https://habr.com/ru/post/436708/ (дата обращения: 25.11.2019).

4. *Морхат П. М.* Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы : автореф. дис. … д-ра юрид. наук. М., 2018. С. 21.

5. *Понкин А. В., Редькина А. И.* Искусственный интеллект с точки зрения права // Вестн. РУДН. Серия: Юридические науки. 2018. С. 94.

6. *Тирранен В. А.* Искусственный интеллект и нейронные сети как инструмент современной киберпреступности // Уголовное право: стратегия развития в XXI веке : материалы XVI Междунар. науч.-практ. конф. (24—25 янв. 2019 г.) М. : РГ-Пресс, 2019. С. 135—140.

7. *H.R.4625* - Future of Artificial Intelligence Act of 2017, 115th Congress [Электронный ресурс]. URL: https://www.congress.gov/bill/115th-congress/house-bill/4625/text (дата обращения: 05.11.2019).

8. *Meško G.* On Some Aspects of Cybercrime and Cybervictimization // European journal of crime, criminal law and criminal justice. Brill Academic Publishers. 2018. № 26. P. 189—199.

9. *Saunders J.* Tackling cybercrime — the UK response // Journal of Cyber Policy, HB Publications, LLC. 2017. № 2 (1). P. 4—15.

V. A. Tyrranen

ARTIFICIAL INTELLIGENCE CRIMES

The article is devoted to current threats to information security associated with the widespread dissemination of computer technology. The author considers one of the aspects of cybercrime, namely crime using artificial intelligence. The concept of artificial intelligence is analyzed, a definition is proposed that is sufficient for effective enforcement. The article discusses the problems of criminalizing such crimes, the difficulties of solving the issue of legal personality and delinquency of artificial intelligence are shown. The author gives various cases, explaining why difficulties arise in determining the person responsible for the crime, gives an objective assessment of the possibility of criminal prosecution of the creators of the software, in the work of which there were errors that caused harm to the rights protected by criminal law and legitimate interests.

Keywords: information security, cybercrime, virtual space, information, artificial intelligence, neural networks.