УДК 343.92

Елена Александровна ЕРАХТИНА,
заведующая кафедрой уголовного процесса, криминалистики и основ судебной экспертизы Юридического института Красноярского государственного аграрного университета, кандидат юридических наук
345nn@mail.ru

Василий Александрович ТИРРАНЕН,
заведующий кафедрой уголовного права и криминологии Юридического института Красноярского государственного аграрного университета, кандидат юридических наук
aw-tirranen@ya.ru

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРОБЛЕМЫ КВАЛИФИКАЦИИ И РАССЛЕДОВАНИЯ

CRIMES MADE WITH THE USE OF ARTIFICIAL INTELLIGENCE: PROBLEMS OF QUALIFICATION AND INVESTIGATION

В статье обсуждаются актуальные угрозы информационной безопасности, порожденные высокотехнологичной организованной киберпреступностью; использование искусственного интеллекта в преступной деятельности, борьба с вирусными многоуровневыми вредоносными компьютерными системами; возникающие на современном этапе развития законодательства и правоприменения проблемы квалификации и эффективного противодействия киберпреступности; причины низкой эффективности расследования киберпреступлений; недостаточное количество специально подготовленных кадров в сфере информационных технологий; неготовность правоприменителя в борьбе с вирусной киберугрозой.

The article discusses current threats to information security generated by high-tech organized cybercrime; the use of artificial intelligence in criminal activity, the fight against viral multilevel malicious computer systems; problems of qualification and effective counter-action of cybercrime arising at the present stage of development of legislation and law enforcement; the reasons for the low effectiveness of cybercrime investigations; insufficient number of specially trained personnel in the field of information technology. unavailability of the law enforcer in the fight against viral cyber threat.

Ключевые слова: *киберпреступность, цифровые технологии, информационная безопасность государства, противодействие киберпреступности, искусственный интеллект, интеллектуальные системы, логика программирования, искусственные нейронные сети, вирусная киберугроза, проблемы расследования.*

Keywords: *cybercrime, digital technologies, state information security, counteraction to cybercrime, artificial intelligence, intelligent systems, programming logic, artificial neural networks, viral cyber threat, problems of investigation.*

Киберпреступность в XXI веке представляет одну их наиболее серьёзных угроз как для информационной безопасности государства, так и для его экономического развития, являясь одной из важнейших проблем современности. [3] Быстрое развитие

цифровых технологий во всех направлениях науки и техники спровоцировало рост организованной высокотехнологичной киберпреступности, отвоевывающей свои позиции в преступном мире.

Успешность борьбы с киберпреступностью во многом определяется эффективностью методики предупреждения преступности и её 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. Киберпреступления, в отличие от «не-цифровых» преступлений, намного сложнее понять и объяснить. [2] В первую очередь это определяется тем, что киберпреступления сами по себе требуют как от преступника, так и от правоохранителя определенной квалификации в сфере информационных технологий. К этой квалификации относятся и понимание логики программирования, и знания в области информационной безопасности, и навыки практического использования 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. Специальные органы многих государств и международных организаций обеспокоены увеличением масштабов киберпреступности, ухудшением последствий для стабильности критически важной инфраструктуры государств и организаций, а также для благополучия людей.

К актуальным угрозам информационной безопасности, порожденным высокотехнологичной организованной киберпреступностью, относятся киберпреступления с использованием искусственного интеллекта, включая искусственные нейронные сети. Использование этого инструмента в преступной деятельности определяет новый уровень угрозы информационной безопасности, что требует готовности правоприменителя в борьбе с такой угрозой.

Для понимания преступлений, совершаемых с использованием искусственного интеллекта, необходимо определить, что понимается под искусственным интеллектом. В широком смысле, применимом к составу преступления, искусственный интеллект – это свойство интеллектуальных систем (в том числе компьютерных программ, включая нейросети) выполнять функции и решать задачи, в том числе специально не оговоренные в системе изначально, обучаться и адаптировать свое поведение под конкретные условия, а также принимать решения исходя из этих условий и поставленных целей.

Человеческий мозг обрабатывает информацию способом, принципиально отличающимся от применяемых обычными компьютерами методов обработки. По существу, мозг представляет собой сложный нелинейный параллельный компьютер: нейроны мозга создают соединения друг с другом в различных комбинациях, при этом количество соединений может составлять до 100 000. Мозг человека организует работу нейронов так, чтобы они выполняли свои функции (распознавание образов, обработка сигналов органов чувств, моторика тела) во много раз быстрее, чем могут позволить современные суперкомпьютеры, за счет выстраивания нелинейных параллельных связей между элементами взаимодействия. Современные системы с искусственным интеллектом способны к обучению на примерах, к самостоятельному обобщению данных, они могут адаптироваться к изменению свойств объекта управления и подстраиваться к внезапно изменившимся условиям внешней среды, при этом обладая высочайшей устойчивостью к повреждению своих элементов при использовании нейросетевой архитектуры. В настоящее время во многих системах для принятия решений и управления процессами используются искусственные нейросети.

До недавнего времени использование искусственного интеллекта в преступной деятельности было ограничено в силу, с одной стороны, недостаточной автоматизации современной жизни, 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 её 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 со смартфона). [1] Ручное управление такой системой человеком-оператором практически невозможно, особенно при большом числе атакуемых одновременно компьютерных систем. Поэтому центр контроля и управления распределенными атакующими объектами должен обладать способностями искусственного интеллекта для проведения полноценной кибератаки с использованием всех доступных возможностей.

Одним из первых примеров использования искусственного интеллекта в широкоформатных кибератаках можно считать вирус CryptoLocker, распространявшийся при поддержке однорангового ботнета Gameover ZeuS, использовавшего зашифрованные каналы связи с центрами контроля и управления. [4] Эта вредоносная система использовала самообучающиеся алгоритмы управления, тип и характер которых в настоящее время достоверно не известен. Обезвреженный в результате операции Tovar ботнет Gameover ZeuS 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.

С уголовно-правовой точки зрения ключевым вопросом использования искусственного интеллекта и нейронных сетей при совершении киберпреступлений остается вопрос определения умысла при совершении деяний, решения о которых принимались искусственным интеллектом самостоятельно, исходя из его адаптивного поведения и способностей к самообучению. На практике данный вопрос пока еще не возникает: у искусственного интеллекта отсутствует возможность совершить эксцесс исполнителя и выйти за пределы ус-

мотрения 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 её обучения. В целом же умысел лица, запускающего работу вредоносной компьютерной системы с использованием искусственного интеллекта, необходимо признать неконкретизированным, поскольку в случае использования самообучающихся систем искусственного интеллекта невозможно спрогнозировать и оценить конкретно причиняемый вред.

Несколько иначе обстоят дела в ситуации, когда за создание системы отвечает одно лицо, а за запуск её в работу – другое, при этом разработчик системы вкладывает в неё некоторые не предусмотренные 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. В таком случае умысел на использование определенного преступного алгоритма у лица, запустившего его в работу, отсутствует, и вменить ему ответственность за нарушение неприкосновенности частной жизни 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 неё такие возможности (в том числе возможность самообучения для сбора информации) и осознававшее то, что в дальнейшем она будет запущена в работу.

Также возможны ошибки в работе вредоносного программного обеспечения, 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 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 неосторожности в форме 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 не представляется возможным: у него в любом случае есть возможность моделирования работы программы перед её запуском, и неосмотрительность по поводу предполагаемых последствий будет последствием его небрежности.

При кажущейся простоте оценки данные выводы связаны с необходимостью практического установления умысла лица, разработавшего или инициировавшего запуск вредоносного программного обеспечения с искусственным интеллектом. В связи с этим при расследовании преступлений, совершенных с использованием вредоносного программного обеспечения, в первую очередь подлежит установлению вопрос наличия в примененном программном обеспечении признаков искусственного интеллекта, что потребует применения специальных знаний для выявления использованных программ, их декомпиляции, а также оценки их архитектуры и методов работы, что подразумевает необходимость привлечения специалистов узкого профиля.

Практический опыт показывает, что при расследовании указанных преступлений основные виды судебной компьютерно-технической экспертизы (аппаратно-компьютерная, программно-компьютерная, информационно-компьютерная) должны использоваться в комплексе.

Найденные экспертом программы с вредоносными (деструктивными) функциями ис-

следуются на стендах, которые моделируют предполагаемые условия их функционирования. Для проведения подобного рода исследований активность найденной вирусной программы исследуют изолированно в виртуальной операционной системе – «песочнице». Виртуализация «песочницы» позволяет эксперту исследовать поведение помещаемого в неё вируса и его воздействие на операционную систему.

При выявлении признаков искусственного интеллекта в коде вредоносных компьютерных программ установлению подлежит также характер его действия, тип используемой архитектуры, признаки самообучаемости и пределы принятия решений, заложенные в такие программы.

Проблема с подобными вирусами заключается в том, что их нужно активировать. После удачной активации он сообщает серверу киберпреступника, что готов к работе, затем получает команду к выполнению задачи. И получается, что если сервер перестал работать, то исследовать вирус проблематично, так как он зашифрован.

Низкая эффективность противодействия киберугрозам и сохранение высокого уровня латентности данных преступлений объясняется также действиями потерпевшей стороны, которая не сообщает (или очень неохотно сообщает) в правоохранительные органы о фактах совершения таких преступлений.

Факторы, влияющие на подобное решение (как правило, это касается юридических лиц):

– потеря клиентов в связи с подрывом деловой репутации (крупные финансовые и промышленные организации);

– опасения, что в ходе расследования выявятся собственные незаконные финансовые операции;

– боязнь должностных лиц предприятий, что в ходе расследования выявится их некомпетентность и профессиональная непригодность, что негативно скажется на их личной карьере;

– ошибочная оценка «ценности» утраченной информации, оценка её без учёта убытков, которые включают в себя неполученные доходы и стоимость восстановления утраченных данных.

В настоящее время на международном уровне разрабатываются предложения по комплексному предупреждению киберпреступности и даже упоминается о необходимости выработки новых национальных и международных правовых или иных мер по борьбе с киберпреступностью, однако до фактического предупреждения внедрения новых технологий при совершении киберпреступлений, в том числе до принятия мер по противодействию распространению искусственного интеллекта во вредоносном программном обеспечении, дело не доходит. При этом, если в ближайшие годы ситуация с запаздыванием создания эффективных мер противодействия новым киберугрозам не изменится, достижения науки в области развития искусственного интеллекта позволят киберпреступности выйти на принципиально новый уровень, позволяющий использовать средства противодействия их выявлению и блокированию.

Библиографический список

1. Тирранен, В.А. Искусственный интеллект и нейронные сети как инструмент современной киберпреступности / В.А. Тирранен // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции (24-25 января 2019 г.) – М.: РГ-Пресс, 2019. – С. 135-140.

2. Mesko, G. On Some Aspects of Cybercrime and Cybervictimization / Gorazd Mesko // European journal of crime, criminal law and criminal justice. Brill Academic Publishers. – 2018. – № 26. – P. 189-199.

3. Saunders, J. Tackling cybercrime – the UK response / Jamie Saunders // Journal of Cyber Policy, HB Publications, LLC. – 2017. – № 2(1). – P. 4-15.

4. Tirranen, V. Cryptoviral Extortion as a Global Problem of Cybersecurity / Vasilii A. Tirranen // Criminal Justice and Security in Central and Eastern Europe. From Common Sense to Evidence-based Policy-making. Conference Proceedings. – Ljubljana, Slovenia, University of Maribor Press, 2018. – P. 548-552.