Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2021. – Т. 7 (73). № 3. Ч. 2. – С. 148-154.

УДК 343.8:004
DOI 10.37279/2413-1733-2021-7-3(2)- 148-154

О ПРИМЕНЕНИИ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ОРГАНИЗАЦИИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Ковтун Ю. А., Лагуточкина А. С.

В статье раскрывается вопрос совершенствования оперативно-розыскного обеспечения противодействия преступности правоохранительными органами за счет применения специализированного программного обеспечения в организации использования искусственного интеллекта.

Развитие информационных технологий требует совершенствования методов и средств осуществления правоохранительной деятельности. Современные реалии сформировали необходимость использование возможностей искусственного интеллекта для решения задач правоохранительной деятельности. В связи с увеличением вычислительных возможностей программно-аппаратных комплексов, в том числе в результате использования графических процессоров и распределенных архитектур вычислительных систем, стало доступным широкое применение машинного обучения на базе множества вычислительных систем, организованных по принципу нейронных сетей.

В качестве эффективного инструмента противодействия преступности правоохранительным органам необходимо иметь в своем арсенале инструменты для осуществления не только мониторинга информационного пространства и получать в режиме реального времени доступ к информации, которая храниться на смартфоне или компьютере пользователя, на облачных хранилищах, в социальных сетях, на встроенных или переносных накопителях. Получать доступ к информации размещаемой, пересылаемой, хранящейся на удаленных серверах, устройствах разрабатываемого лица посредством удаленного мониторинга, иметь возможность обработки больших объёмов данных и решения сложных задач быстрее, чем существующие сейчас традиционные алгоритмы. Для получения необходимых данных требуется использование специализированного информационного программного обеспечения сетевой среды, направленного на решение задач раскрытия и расследования преступлений.

Ключевые слова: специализированное программное обеспечение, информация, технологии, правоохранительная деятельность, искусственный интеллект.

Эволюция развития от примитивных компьютерных сетей и компьютерных устройств до современных высокотехнологических сетей и устройств произошла в короткие сроки [1]. Информационные технологии и техника являются одной из основных характеристик современного информационного общества. Использование информационных технологий играет важную роль в обеспечении возможности информационного взаимодействия между членами общества. Современное информационное пространство позволяет реализовать новые технологии по созданию, передаче, хранению, внесению изменений, накоплению массивов информации, баз данных. Современные реалии показали, что все правоохранительные органы мира оказались мало подготовленными к противодействию преступлениям совершаемых в цифровом пространстве или с использованием возможностей цифрового пространства. Классические методы получения и фиксации информации оказались не действенными. Развитие информационных технологий требует совершенствование методов и средств осуществления правоохранительной деятельности направленных на раскрытие и расследование преступлений, предупреждение преступлений. Востребованы

оказались методы удаленного получения и фиксации доказательств без привязки к территориальной принадлежности правоохранительных органов.

Отставание в развитии методов и средств правоохранительных органов от темпов развития процесса информатизации общества, приводит к тому, что преступления, совершаемые посредством современных технологий, в сетевых инфраструктурах, остаются безнаказанными, что естественно стимулирует их продолжение и увеличение их количества. Проведение следственных действий и оперативно-розыскных мероприятий с использованием информационного пространства сети Интернет уже давно не являются экстраординарными и используются при раскрытии и расследовании преступлений правоохранительными органами всех стран.

В работе использованы различные общенаучные приемы и способы логического познания: анализ и синтез, системный, функциональный и формально-логический подходы. Формированию выводов способствовало применение метода контент-анализа, формально-юридического и сравнительно-правового методов.

Количество преступлений, совершаемых в сфере информационно-коммуникационных технологий, за последние три года увеличилось в шесть раз. Для эффективной работы по противодействию преступлениям в этой сфере правоохранительным органам необходимо иметь возможность получать доступ к информации размещаемой, пересылаемой, хранящейся на удаленных серверах, устройствах разрабатываемого лица посредством удаленного мониторинга. Данные, получаемые посредством цифровых технологий, обладают высокой степенью информативности. Получение ее возможно без привязки к месту нахождения разрабатываемого лица в режиме реального времени. Но получение этой информации возможно только при наличии соответствующего программного обеспечения и квалифицированных специалистов, работающих со специализированным цифровым программным обеспечением. Однако, в настоящее время, уровень обеспечения специализированными программными продуктами в правоохранительных органах России не соответствует современным требованиям [2].

Как известно, любая современная компьютеризированная техника не может работать без программного обеспечения. Компьютерная техника без программного обеспечения – бесполезна. Немыслимое количество программ обеспечивает функционирование современной вычислительной техники. Известно, что все программное обеспечение можно разделить на: системное, вспомогательное, специальное. Среди системного обеспечения наиболее популярные «Windows», «MacOS», «Linux», «Android», «iOS».

Вспомогательное программное обеспечение синхронизирует работу установленного оборудования с имеющейся операционной системой в необходимом для пользователя режиме. Достаточно часто в обиходе их называют «драйверами», «прога», «водила», «таблетка», «парус».

Специализированное программное обеспечение представляет собой совокупность программ, непосредственно реализующих алгоритмы решения функциональных задач [3]. Данные программы устанавливаются для работы с компьютеризированным оборудованием в индивидуальном направлении деятельности пользователя. Данное программное обеспечение производят специализирующиеся на производстве IT-технологий компании самостоятельно или

в соответствии с договорными обязательствами, где заказчиками выступают заинтересованные организации, компании, холдинги, а также государственные органы. Кроме основных производителей программного обеспечения, таких интернет-гигантов как International Business Machine или IBM, Microsoft, Oracle, Kaspersky, Mail.ru Group, не запрещается создание программ и физическим лицам с некоторыми оговорками в пользу обязательных налоговых платежей, если эта деятельность приносит доход, а также ограничением этой деятельности в условиях действия законодательства страны. Правоохранительные органы все более активно используют специализированное программное обеспечение, позволяющее следить за пользователями соцсетей, в том числе читать их личные сообщения, собирать данные о геолокации и анализировать связь между разными пользователями**,** программное обеспечение способное разблокировать модели телефонов с операционной системой Android и другие.

Преступники, как и остальная часть граждан активно пользуются для общения социальными сетями, мессенджерами контроль за которыми в настоящий момент имеет множество тонкостей. Одной из глобальных проблем является то, что ряд программ имеют зарубежное происхождение, и географическое нахождение серверов и облачных хранилищ находятся за пределами Российской Федерации. В условиях политической нестабильности между государствами, возникают трудности в обеспечении международной безопасности. Члены международной коллективной безопасности посредством лоббирования и оказывания политического давления, а также введением санкций, ограничивают допуск и предоставление сведений по международным запросам правоохранительных органов из массива накапливаемых сведений, в части обеспечения функционирования программного продукта на международном уровне.

Выходов из этой ситуации два. Первый – это взаимодействие с зарубежными правоохранительными органами. Это необходимо в связи с увеличением вычислительных возможностей программно-аппаратных комплексов, в том числе в результате использования графических процессоров и распределенных архитектур вычислительных систем. И возможностью применение машинного обучения на базе множества вычислительных систем, организованных по принципу нейронных сетей. Что обеспечит скорость получения информации и увеличит объем обрабатываемой информации. Что позитивно скажется на деятельности всех взаимодействующих правоохранительных органов. Полноценная реализации обмена правоохранительными органами информаций посредством нейросетевых технологий приведет к изменениям прорывного характера. Применение технологии блокчейна в международном формате позволит создать базу данных правоохранительных органов, сохраняющая постоянно увеличивающийся объём информации в виде отдельных блоков, имеющих данные о предыдущем блоке и сохраняющие данные о времени их создания. Устройства хранения в данной системе будут иметь сервера в различных государствах. Наиболее популярное и эффективное направление развития блокчейна это реестр хранения данных. Многие государства уже внедряют эти системы. Правительство Бразилии экспериментирует с uPort. Министерство планирования, бюджета и управления Бразилии тестирует независимое блокчейн-приложение uPort для идентификации личности, разработанное ConsenSys. Созданная на основе Ethereum платформа предоставляет возможность пользователям редактировать соб-

ственные профили, а Министерство будет проверять легитимность загруженных личных документов. Внедрение современной технологии блокчейна, в деятельности правоохранительных органов позволит оперативно получать информацию необходимую для раскрытия и расследования преступлений и предотвращения преступлений. Внедрение этой технологий в правоохранительную деятельность позволит значительно сократить сроки получения информации и получать ее в режиме реального времени и из любой точки мира.

Второй – это создание и использование национального программного обеспечения, цифровые мощности которого находятся в пределах государства. Во-первых, это дает возможность полного контроля за данными пересылаемыми посредством национального программного обеспечения. Что безусловно возможно только при создании дополнительного специализированного информационного программного обеспечения сетевой среды, направленного именно на решение задач правоохранительных органов. Вопросы необходимости разработки нового или совершенствование ранее используемого программного обеспечения должны решаться преимущественно научно-исследовательскими организациями системы правоохранительных органов по результатам мониторинга возможностей информационных технологий и сопоставления имеющегося программного обеспечения. Для успешного выполнения своих задач правоохранительные органы должны иметь возможность получать в режиме реального времени доступ к информации, которая храниться на смартфоне или компьютере пользователя, на облачных хранилищах, в социальных сетях, на встроенных или переносных накопителях. Говоря о возможных злоупотреблениях при осуществлении допуска к информации пользователей со стороны правоохранительных органов (незаконного и необоснованного ее получения) то напомним, решение о проведения оперативно-розыскных мероприятий, следственный действий, ограничивающих право не неприкосновенность переписки, возможно только по судебному решению [4]. Данный алгоритм принятия решения позволяет использовать данные возможности в соответствии с требованиями Конституции Российской Федерации и допускать только законное и обоснованное ограничение конституционных прав личности. Во-вторых, создание и использование собственного программного обеспечения решает задачу укрепления национальной безопасности России, ввиду ограниченных возможностей воздействия на российские программы иностранных спецслужб. Исходя из поступающих данных, доля зависимости России от программного обеспечения иностранного производства в 2015 г. достигала 80–90%, в 2019 г. уже достигала 75%, а с 1 января 2021 г. в некоторых сферах функционирования предприятий, владеющих «критической информационной инфраструктурой» (КИИ) Минкомсвязи России рекомендовало полностью перейти на российское программное обеспечение [5]. В связи с чем было решено провести поэтапное импортозамещение иностранного программного обеспечения, на российского производителя и поставлена задача по созданию отечественного продукта способного обеспечить информационную безопасность государства. В части обеспечения этого процесса был принят ФЗ от 29.06.2015 N188-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и ст. 14 ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», который обеспечивает приоритет российского программного продукта перед иностранным при участии в госзакуп-

ках, а Постановление правительства РФ от 16 ноября 2015 г. №1236 «Об установлении запрета на допуск иностранного программного обеспечения при закупках для государственных и муниципальных нужд» внесло разъяснения и определило механизм импортозамещения цифровой продукции [6].

В настоящий момент применение и использование специализированного программного обеспечения для правоохранительных органов имеет место на практике.

Так, в ГУ МВД по Свердловской области активно применяется аппаратно-программный комплекс (АПК) «Зеус», который был разработан по заказу МВД России. Данный АПК осуществляет мониторинг сетевой активности пользователей социальных сетей, в частности: выявляет незаконно размещенный контент на страницах социальных сетей; выявляет лиц, от которых можно ожидать преступлений, формирует наиболее активных пользователей в исследуемых условиях; определяет связи по социальным направлениям и т. д.

Многие возможности, которые дает представленная программа, возможно реализовать путем мониторинга открытых данных в социальных сетях. Но некоторые данные которые необходимы для полноценной работы программы можно реализовать только при получении доступа к закрытой информации социальных сетей. За время использования системы она себя достаточно хорошо зарекомендовала и позволила получить информацию, которая была использована при раскрытии преступлений и расследовании уголовных дел [7].

Вехой применения цифровых программ в деятельности правоохранительных органов на сегодняшний день является использование нейросетевых технологий (искусственного интеллекта). Исследуя перспективы применения нейросетевых технологий в деятельности правоохранительных органов важно отметить, что применение искусственного интеллекта весьма существенно повлияет на формирование новейшего направления противодействия преступлениям и в части их предупреждения и пресечения [8]

В ряде стран таких как Китай, Франция, США возможности нейросетей и программного обеспечения в правоохранительной деятельности уже внедряются и используются [9]. Следует учитывать, что даже отдельные элементы, внедряемые в систему искусственного интеллекта, могут иметь существенные недостатки. Комиссар Совета Европы (СЕ) по правам человека Д. Миятович в октябре 2019 г. на конференции, посвящённой проблемами цифровых технологий в правоохранительной деятельности, напомнила, что на конечные результаты системы искусственного интеллекта влияют разработчики этого программного продукта. Они могут иметь свои вкусовые предпочтения или предрассудки, которые будут интегрированы в деятельность правоохранительных органов, что изначально может привести к дискриминации деятельности правоохранительных органов [10].

Избранный курс о создании искусственного интеллекта в МВД уже декларированы в обществе. Так, известно, что по заказу МВД России разрабатывают Федеральную информационную систему биометрических учетов (ФИСБУ). Данная система до конца 2021 г. будет внедрена в работу МВД и нацелена на поиск подозреваемых, преступников и разыскиваемых лиц с помощью установленных в городе камер видеонаблюдения.

Исследуется возможность применения искусственного интеллекта в обработке данных системы ФИСБУ, для распознавания человека по изображению лица, голо-

са, татуировкам на открытых частях тела, радужной оболочке глаза и иным идентифицирующим признакам человека. Тестирование данной системы будет проведено в части использования уже существующей сети видеоконтроля «Безопасный город».

Кроме того, 12 ноября 2019 г. на стратегической сессии Правительства РФ, для МВД России утвердили проект по внедрению искусственного интеллекта в целях выявления серийных преступлений и поиска преступников. В алгоритме внедрения искусственного интеллекта указано, что в 2020 г. МВД начнет подготовку технических заданий на проведение научно-исследовательских работ по внедрению технологий искусственного интеллекта в работе полиции, а в 2023 г. приступит к опытно-конструкторским работам по созданию конкретного софта — для поиска серийных преступников и для «определения индивидуальных анатомических признаков человека, полученных из биологического материала с мест совершения преступлений».

Так, в начале третьего тысячелетия мы наблюдаем кардинальные преобразования в сфере информационных технологий в информационном пространстве. Особенностью современных преступлений является то, что при их использовании преступникам необходимо использовать возможности информационных технологий для планирования преступлений, координации действий, осуществления платежей, переводов или вывода денежных средств, даже при совершении преступлений не в цифровом пространстве. Выбор средств получения и передачи информации используемых в преступных целях посредством современных технологий разнообразен. Сейчас при совершении преступлений сообщники могут находиться за сотни, а то и тысячи километров друг от друга, а иногда и от места совершения преступления. В таких условиях проведение необходимых оперативно-розыскных и процессуальных действий требуют совместных согласованных действий правоохранительных органов различных государств В качестве эффективного инструмента противодействия преступности правоохранительным органам жизненно важно иметь в своем арсенале инновационные, эффективные инструменты мониторинга информационного пространства с использованием возможностей нейросетевых технологий (искусственного интеллекта). И уже давно назрела необходимость тесной интеграции правоохранительных органов не только соседних государств, но и тех, кто не имеет общих границ. Перед угрозами террористических преступлений иных опасных проявлений преступности нужна сплоченная командная работа без политических вкусов и предпочтений отдельных государств. Конечно сейчас существует международная уголовная полиция Интерпол куда входит 194 страны, но к сожалению, на работу и взаимодействие существенное значение оказывает политическая повестка. Обеспечение безопасности граждан основная задача любого государства, у преступности нет национальности, расы, вероисповедания и борьба с ней вне политической плоскости. Только комплексная международная система безопасности позволит противостоять организованной международной преступности. Объединение информационных баз различных государств в единую международную систему позволит противостоять современным вызовам преступности.

Список литературы:

1. CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment#o.

2. Загайнов В.В., Кононов Ю.Н. Оперативно-аналитическая работа как основа оперативно-розыскной деятельности в современных условиях. Вестник Восточно-Сибирского института Министерства внутренних дел России. 2017. № 1 (80). С. 37-46.
3. Классификация программного обеспечения профессионально-ориентированных ИС. [Электронный ресурс] https://studopedia.ru/12_92697_zadachi-upravleniya-gornim-davleniem-i-osnovnie-printsipi.html/ (1.03.2021).
4. Климов Д.А., Климов А.А. Использование результатов ОРД в качестве ориентирующей информации по делам о преступлениях в сфере экономики. В книге: Борьба с преступностью: теория и практика Материалы II Международной научно-практической конференции. 2014. С. 124-125.
5. Правительство «поздравило» Windows с юбилеем. [Электронный ресурс] http://rusplt.ru/society/society_19825.html/ (1.03.2021).
6. Итоги 2017 года: программное обеспечение. [Электронный ресурс] https://3dnews.ru/963329/ (1.03.2021).
7. За вами следит «Зеус». [Электронный ресурс] https://www.znak.com/2016-07-27/mvd_obnarodovalo_dokumenty_o _slezhke_za _polzovatelyami_socsetey (1.03.2021).
8. Robot Law. Ed. by Calo R., Froomkin A.M., Kerr I. Cheltenham, UK. Northampton, MA, USA. Edward Elgar Publishing. 2016.
9.Marina Nagornaya. Lawyers and lawyers about artificial intelligence in legal proceedings. https: //www.advgazeta.ru/novosti/advokaty-i-yuristy-ob-iskusstvennom-intellekte-v-sudoproizvodstve/ (03.03.2021).
10. Justice in Europe facing the challenges of digital technology. https: //www.coe.int/en/web/commissioner/-/justice-in-europe-facing-the- challenges -of-digital-technology

Y. A. Kovtun, A. S. Lagutochkina. On the use of specialized software by law enforcement agencies in the organization of the use of artificial intelligence // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2021. – T. 7 (73). № 3. – P. 148-154.

The article reveals the issue of improving the operational and investigative support for countering crime by law enforcement agencies through the use of specialized software in the organization of the use of artificial intelligence. The development of information technologies requires the improvement of methods and means of law enforcement activities. Modern realities have formed the need to use the capabilities of artificial intelligence to solve law enforcement tasks. Due to the increase in the computing capabilities of software and hardware complexes, including as a result of the use of graphics processors and distributed computing system architectures, a wide application of machine learning based on a variety of computing systems organized on the principle of neural networks has become available. As an effective tool for countering crime, law enforcement agencies need to have in their arsenal tools for not only monitoring the information space and getting real-time access to information that is stored on a user's smartphone or computer, on cloud storage, in social networks, on built-in or portable storage devices. Get access to information posted, sent, stored on remote servers, devices of the person being developed through remote monitoring, be able to process large amounts of data and solve complex problems faster than the traditional algorithms currently existing. To obtain the necessary data, it is necessary to use specialized information software of the network environment aimed at solving the tasks of solving and investigating crimes.

Key words: specialized software, information, technologies, law enforcement, artificial intelligence.

Spisok literatury

1. CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment
2. Zagajnov V.V., Kononov YU.N. Operativno-analiticheskaya rabota kak osnova operativno-rozysknoj deyatel'nosti v sovremennyh usloviyah. Vestnik Vostochno-Sibirskogo instituta Ministerstva vnutrennih del Rossii. 2017. № 1 (80). S. 37-46.
3. Klassifikaciya programmnogo obespecheniya professional'no-orientirovannyh IS. [Elektronnyj resurs] https://studopedia.ru/12_92697_zadachi-upravleniya-gornim-davleniem-i-osnovnie-printsipi.html/ (1.03.2021).
4. Klimov D.A., Klimov A.A. Ispol'zovanie rezul'tatov ORD v kachestve orientiruyushchej informacii po delam o prestupleniyah v sfere ekonomiki. V knige: Bor'ba s prestupnost'yu: teoriya i praktika Materialy II Mezhdunarodnoj nauchno-prakticheskoj konferencii. 2014. S. 124-125.
5. Pravitel'stvo «pozdravilo» Windows s yubileem. [Elektronnyj resurs] http://rusplt.ru/society/society_19825.html/ (1.03.2021).
6. Itogi 2017 goda: programmnoe obespechenie. [Elektronnyj resurs] https://3dnews.ru/963329/ (1.03.2021).
7. Za vami sledit «Zeus». [Elektronnyj resurs] https://www.znak.com/2016-07-27/mvd_obnarodovalo_dokumenty_o _slezhke_za _polzovatelyami_socsetey (1.03.2021).
8. Robot Law. Ed. by Calo R., Froomkin A.M., Kerr I. Cheltenham, UK. Northampton, MA, USA. Edward Elgar Publishing. 2016.
9. Marina Nagornaya. Lawyers and lawyers about artificial intelligence in legal proceedings. https: //www.advgazeta.ru/novosti/advokaty-i-yuristy-ob-iskusstvennom-intellekte-v-sudoproizvodstve/ (03.03.2021).
10. Justice in Europe facing the challenges of digital technology. https: //www.coe.int/en/web/commissioner/-/justice-in-europe-facing-the- challenges -of-digital-technology

.