

СУЩНОСТЬ, ФОРМИРОВАНИЕ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Лагуточкин А. В.

Крымский филиал Краснодарского университета МВД России

В статье раскрываются вопросы формирования и перспектив использования нейросетевых технологий (искусственного интеллекта) подразделениями органов внутренних дел, осуществляющими оперативно-розыскную деятельность.

Использование нейросетевых технологий выступает при этом одной из важнейших предпосылок структурного построения безопасности государства, где искусственный интеллект приобретает статус инструмента в достижении первоочередных целей правоохранительных органов.

Избрав цель занять достойное место среди ведущих стран мира в области развития информационного общества, наша страна активно развивает собственную информационную и телекоммуникационную инфраструктуру. Можно констатировать, что от декларирования намерений в указанной сфере государство перешло к конкретным действиям, и на этом пути уже достигнуты заметные результаты.

Применение искусственного интеллекта в правоохранительной сфере препределяет инновационные подходы к выявлению, предупреждению, пресечению и раскрытию преступлений на территории Российской Федерации.

Ключевые слова: искусственный интеллект, нейросети, оперативно-розыскная деятельность, оперативно-розыскные мероприятия, учеты.

Последние тенденции в развитии науки и техники позволяют говорить о том, что человечество стоит на пороге новой эры – эры искусственного интеллекта: технологии служат на благо жизни человека, а такие термины как «нейросети» и «эволюционные алгоритмы» не кажутся научно-фантастическими, а, напротив, весьма применимы в обыденной жизни. Однако любое изобретение должно служить во благо и удовлетворять конкретные потребности личности, общества, государства. Потому внедрение инновационных разработок в отдельные сферы государственного строительства считается весьма приоритетным направлением развития науки и техники.

Реалии современного мира позволяют говорить о значительной степени информатизации, а также цифровизации общественных процессов: увеличиваются информационные блоки, ускоряются информационные связи. Для обработки имеющегося объема данных сегодня весьма широко используются технологии, связанные с самообучающимися системами искусственного интеллекта. Как писал Н. Ротшильд: «Кто владеет информацией, тот владеет миром», - отсюда вполне очевиден вывод, что системы обработки информации с помощью нейронных сетей являются весьма актуальными и будут сохранять данное свойство до тех пор, пока человек будет заинтересован в процессах обработки, хранения и передачи информации.

Как известно мозг человека способен воспринимать и обрабатывать поступающий информационный поток в достаточно сложном процессе работы нейронных связей и близко не может быть похож на компьютерный метод обработки информации. Однако, человеческий мозг может напоминать сложный нелинейный параллельный компьютер в котором нейроны мозга создают соединения друг с другом в

различных комбинациях, при этом количество соединений может составлять до 100 000. Человеческий мозг способен организовать функционирование нейронов так, чтобы они выполняли свою работу (обработка сигналов органов чувств, распознавание образов, моторика тела) во несколько раз быстрее, чем могут позволить современные суперкомпьютеры, например, за счет выстраивания нелинейных параллельных связей между элементами взаимодействия. В то же время, современные компьютеры, с нейросетевыми связями (искусственным интеллектом) выполняют функцию, связанную с обучением на примерах, на закладываемых алгоритмах, способны к самостоятельному анализу 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.

Так, весьма значительных успехов, как в теоретическом, так и в практическом исследовании искусственного интеллекта добилась Япония, где в 2000-е годы компьютеризация достигла определённых вычислительных возможностей. Это в свою очередь, позволило выработать методы «машинного обучения» - такие методы, которые используют математические модели исчисления, предназначенные для аналитической обработки данных об определенных явлениях. И что очень важно, обучение искусственного интеллекта на основе выявленных таким образом тенденций и принятие решений, а также прогнозирование на основе результатов этого обучения [5].

Широта применения искусственного интеллекта весьма разнообразна – это семантический поиск, экспертные системы и системы поддержки принятия решений, распознавание текста и речи, предсказание курсов акций, анализ текстов, системы безопасности. Нейросети особенно эффективны там, где нужно подбие человеческой интуиции, в частности к таким задачам относится принятие решений.

На сегодняшний день искусственный интеллект становится весьма перспективной инвестицией для таких корпораций, как Яндекс, Google, Yahoo, DWANGO, Preferred Networks, а также для таких крупных предприятий, как Toyota, FANUC и многих других.

Перспективы развития искусственного интеллекта в контексте рыночной экономики и коммерческих интересов вполне очевидны. На наш взгляд, наиболее актуальными на сегодняшний день являются вопросы внедрения искусственных нейронных сетей в деятельность учреждений и организаций социальной сферы, а также государственных органов. Обусловлено это исключительно утилитарными потребностями государства и общества, которые могут быть удовлетворены гораздо меньшим количеством затрачиваемых на это ресурсов.

Говоря о сфере применения нейросетей, стоит отметить, что на сегодняшний день она весьма обширна. Более того интерес к искусственному интеллекту возрастает в геометрической прогрессии. Потому считаем, что выбранная нами тематика научного исследования наиболее актуальна и соответствует потребностям современного общества.

Для того, чтобы дать понятие искусственной нейросети, используемой в оперативно-розыскной деятельности, считаем необходимым отталкиваться от функционального инструментария искусственного интеллекта.

Отталкиваясь от целей и задач борьбы с преступностью, мы можем перечислить те функции, которые могли бы реализовать нейросети при осуществлении оперативно-розыскной деятельности. Так, например, к их числу можно отнести: своевременное и наиболее полное документирование преступной деятельности лиц, подозреваемых в совершении преступления; эффективность планирования и проведения оперативно-розыскных мероприятий (а также оперативно-поисковых мероприятий по выявлению лиц, совершивших преступление, розыску преступников); достаточный уровень информационного обмена между оперативными подразделениями и службами в целях повышения их мобильности и качества взаимодействия при осуществлении оперативно-розыскной деятельности; прогнозирование и планирование при осуществлении оперативно-розыскной деятельности субъектами управления в целях оптимизации служебного процесса и экономии трудовых ресурсов и др.

Моделирование решаемых задач дает основание говорить о необходимости в перспективе использования субъектами ОРД искусственных нейросетей как средства ОРД. Закономерным будет тезис о том, что искусственный интеллект может стать комплексным средством ОРД, объединив в себе природу учетов и технических средств, используемых для решения задач ОРД [6].

На наш взгляд, данный подход вполне рационален. Использование искусственного интеллекта имеет значительное количество преимуществ, среди которых, например:

1) экономия времени, сил и средств ОРД.

В контексте постоянно меняющейся оперативной обстановки весьма актуальными становятся вопросы рационального использования сил и средств. Так, например, нейросеть посредством постоянного мониторинга и контроля за состоянием оперативной обстановки, а также имеющихся в ее распоряжении баз данных позволяет спрогнозировать какое ОРМ и когда необходимо осуществить в целях пресечения противоправной преступной деятельности лица. За счет чего повышается результативность проведения ОРМ, так как принятое системой решение основано на синхронизированном анализе взаимосвязанных данных.

2) полнота и своевременность документирования преступной деятельности.

Благодаря тому, что мониторинг состояния оперативной обстановки искусственной нейросетью ведется постоянно, исключается вариант, что какое-либо совершенное противоправное деяние окажется неучтенным и незамеченным для оперативных подразделений.

Таким образом, будет решаться еще и задача контроля за учетно-регистрационной деятельностью органов внутренних дел. Более того, если информация, полученная в рамках мониторинга нейросетью, после соответствующей санкции территориального органа внутренних дел будет зарегистрирована в КУСП, то нейросеть способна обработать и включить уже обработанные данные в соответствующую автоматизированную базу данных. Тогда оперативность отражения оперативно-значимой информации в учетах с целью информирования иных оперативных подразделений и служб будет обеспечена.

3) решение кадрового вопроса, а также стабилизация служебной нагрузки на оперативного сотрудника.

Внедрение искусственного интеллекта в деятельность оперативных подразделений позволит сэкономить трудовые ресурсы для принятия наиболее значимых управленческих решений. Более того чем выше объем данных, на основе которых формируются самообучающиеся алгоритмы нейросети, тем выше качество принимаемых ею решений и рекомендаций, имеющих ориентирующее значение при планировании оперативно-розыскной деятельности. Данный факт может иметь определяющее значение особенно в случаях, когда объем территории оперативного обслуживания, закрепленного за соответствующим территориальным органом, весьма велик и имеется некомплект сотрудников в оперативном подразделении.

Так или иначе, решение отдельных тактических или оперативно-служебных задач при помощи искусственных нейронных сетей позволяет решить одну глобальную проблему – это повешение защищенности государства и общества от противоправных посягательств. Ведь именно эту цель должна преследовать деятельность всех правоохранительных органов государства, включая оперативные подразделения и службы.

4) сокращение коррупционных влияний в борьбе с преступностью.

Для искусственного интеллекта, в соответствии со ст. 8 ФЗ «Об ОРД» – пол, национальность, расовая принадлежность и иные указанные характеристики не являются препятствием к проверке и анализу данных на предмет участия в преступной и иной противоправной деятельности. Кроме того, должностное положение фигуранта или степень участия лица в обеспечении правопорядка или судебной деятельности не сможет оказывать воздействие на декларирование предложений искусственного интеллекта, в части исполняемых им предназначений. Это позволит беспринципно подходить ко всем лицам, находящимся на территории Российской Федерации, равных в правах и обязанностях перед законом. В случаях, если фигурант подпадает под действие федеральных законов как спецсубъект, имеющий особый правовой статус (депутаты, судьи и др.), искусственный интеллект вправе затребовать предварительные (разрешающие) материалы для обеспечения доступа к результатам своей работы.

Среди основных тенденций развития оперативно-розыскной деятельности наряду с нормативно-правовым совершенствованием глобальным направлением остается технический прогресс. Он осуществляется за счет внедрения в жизнь человека все более новых образцов техники разрабатываемых на инновационных принципах работы, являющихся неотъемлемой частью жизнедеятельности социума.

В свое время подобными технически революционными изобретениями являлись компьютеры и сетевые возможности их использования, сотовая связь, позволяющая в разы увеличить коммуникативность общества и развивающая иные сервисные технологии данного процесса.

Искусственный интеллект в ближайшем будущем однозначно займет свою нишу в общественной востребованности, как для социальной сферы, так и в экономике, особенно, в части потребления и т.д. Для того, чтобы программы искусственного интеллекта могли полноценно работать, должны быть сформированы подразделения, на которые будет возложена ответственность за развитие технического обеспечения рабочих процессов [7].

В правоохранительной деятельности использование нейросетевых технологий – новейшая веха, которая позволит на «революционном уровне» пересмотреть и усовершенствовать работу органов внутренних дел. Остается много вопросов применения нейросетевых технологий: их техническое обеспечение, организация и применение в решении конкретных правоохранительных задач, в т.ч. задач оперативно-розыскной деятельности.

Существование искусственного интеллекта абсолютно невозможно без исходной информации, банков данных или учетов формируемых различной категорией субъектов. Данные банки информации можно разделить на следующие категории: государственные банки данных (учеты органов внутренних дел; учеты государственных организаций); негосударственные банки данных.

В целом для формирования учетов имеется ряд требований: 1) точность – каждый объект должен быть подробно описан по всем присущим ему одному признакам; 2) полнота и достоверность – должны быть учтены все объекты, подлежащие учету; 3) своевременность – необходимо своевременно выявлять и регистрировать объекты, подлежащие учету; 4) целенаправленность – четкое разграничение сведений в зависимости от информационной потребности субъектов оперативно-розыскной деятельности и выбор оптимального управленческого уровня системы органов внутренних дел для организации учета; 5) простота и удобство – наличие унифицированных, несложных для заполнения, но охватывающих все признаки объекта учета документов, карточек; а также широкое применение автоматизированных поисковых систем; 6) Комплексность – сочетание логически увязанных сведений, полученных из различных источников; 7) Ценность (полезность) – из всего существующего разнообразия информации должна отбираться только та, которая будет способствовать эффективному решению задач оперативно розыскной деятельности.

Как известно учеты органов внутренних дел – это система регистрации, сосредоточения, классификации, хранения данных о лицах, предметах, событиях по их признакам, предназначенная для эффективного информационного обеспечения деятельности ОВД и их оперативных подразделений в целях предупреждения, раскрытия, расследования преступлений, розыска скрывшихся преступников и иных категорий разыскиваемых лиц.

Отдельно хотелось бы отметить учеты государственных органов, не относящихся к правоохранительной деятельности. Основным источником информации для правоохранительной деятельности являются медицинские учреждения.

Следует иметь в виду, что в последнее время многие крупные медицинские учреждения переходят на автоматизированный учет пациентов и это положительно соотносится с внедрением нейросетевых технологий.

Отдельно необходимо остановиться на негосударственных базах данных формируемых предприятиями организациями учреждениями в части осуществления предпринимательской и иной деятельности, в том числе объединении осуществляющих некоммерческую деятельность.

Формируемые информационные системы позволяют оптимизировать деятельность юридических лиц, формируя сведения о клиентах, о динамике спроса, ценообразовании и т.д.

Для правоохранительных органов эти сведения не менее интересны в части осуществления контроля в отношении лиц подготавливающих, совершающих, совершивших преступления, а также выявления сопутствующей информации, связанной с выявлением свидетелей или очевидцев преступлений или иной информации имеющей доказательственное значение.

Так, приобретение и доставка гражданам коммерческой организацией через интернет-магазин зарубежных представителей предметов могущих подпадать под ст. 138.1. УК РФ (незаконный оборот специальных технических средств, предназначенных для негласного получения информации) образует уже состав преступления и взаимодействие в этой части с подобными коммерческими структурами является обязательным [4].

Особое внимание следует уделить формируемым базам данных в банковской сфере. Коммерческие банки вкладывают в обеспечение собственной безопасности огромные суммы денежных средств, в разработку информационного контента, а также в передовые технологии. Сегодня практически большинство кредитов выдается гражданам с обязательной процедурой идентификации личности Face-ID. С учетом развития в МВД России технологии распознавания лиц, полученные сведения из негосударственных органов достаточно дополнили имеющийся банк данных. Это позволило более широко применять полученные сведения.

Существует отдельная отрасль, с которой правоохранительные органы обязаны осуществлять взаимодействие – организации предоставляющие услуги телекоммуникационных технологий и сотовой связи. Не является секретом то, что практически все оперативно-розыскные мероприятия ограничивающие права и свободы человека и гражданина преимущественно осуществляются совместно с рассматриваемыми организациями. Банки данных формируемые этими организациями являются весьма «ценным» контентом для оперативно-розыскной деятельности, а принятые федеральные законы («законы Яровой» [3]) обязывают операторов связи обеспечивать хранение звонков и сообщения абонентов за период, определяемый Правительством Российской Федерации (но не более, чем за 6 месяцев) в соответствии с 64-й статьей федерального закона «О связи», а информацию о фактах приема, передачи, доставки и обработки сообщений и звонков – 3 года [2].

Представленные для хранения данные являются весьма ценными данными для правоохранительной деятельности, не только ввиду характера передаваемой информации, но и в части, выявления уникальности голоса для последующей идентификации человека. Эти сведения расширяют возможности информационных баз для искусственного интеллекта. Рассмотренные выше информационные ресурсы, это всего лишь малая часть данных, которые необходимо использовать для обработки с использованием нейросетевых технологий.

Таким образом, возможности искусственного интеллекта позволяют решать вопросы, возникающие при решении задач ОРД, наряду с другими средствами – учеты, технические средства, служебные собаки и иные средства, используемые при осуществлении оперативно-поисковых и оперативно-розыскных мероприятий. Потому совершенствование технической составляющей деятельности оперативных подразделений кажется нам наиболее обоснованным и необходимым способом

упредить преступную деятельность еще на этапе подготовки к совершению преступления.

На сегодняшний день особое место среди наиболее посещаемых онлайн-платформ заняли социальные сети, используемые в качестве особых ресурсов, обеспечивающих контакт между людьми.

Крупнейшей социальной сетью отечественного сегмента Интернета является «ВКонтакте» с целевой аудиторией более 90% юношей и более 94% девушек. При этом в последнее время среднестатистический интернет-пользователь не ограничивается поисковой системой или почтой и, как правило, подписан сразу на несколько социальных сетей («ВКонтакте» – 90-93% несовершеннолетних пользователя, Facebook – 13-15%, «Одноклассники» – 16%, Twitter – 10%, Instagram – 54%), новостные сайты, блоги, тематические и справочные проекты. Кроме того, для пользователя открываются значительные возможности для свободного взаимодействия в онлайн-режиме не только посредством социальных сетей, но и через ICQ, Messenger, Skype, Viber, Jabber, WhatsApp и т. д. [5].

Вполне очевидно, что социальная среда указанных платформ не только не препятствует, но и во многих случаях способствует криминогенному влиянию на несовершеннолетних. Криминогенный потенциал контента социальных сетей прогрессирует благодаря таким свойствам, как общедоступность, открытость, востребованность, децентрализованность и анонимность.

Комплексное сочетание указанных качеств зачастую негативно воздействует на несовершеннолетних пользователей, ведь способствует латентному информационно-психологическому воздействию на эмоционально-поведенческое и когнитивное состояние неограниченного количества пользователей, формирует и изменяет их социальные установки, деформирует правосознание и поведение несовершеннолетних. Поэтому вследствие негативного воздействия контента социальных сетей дети и подростки становятся не только потерпевшими от преступлений, но иногда и сами превращаются в источник повышенной опасности.

Практика показывает, что социальные сети в настоящее время представляют уникальные возможности для распространения негативной информации; организации сообществ противоправного характера; коммуникации с целью вовлечения в осуществление преступных деяний; обмена преступным опытом. Угрозы, преследующие несовершеннолетних в соцсетях многогранны и разнообразны [3].

Отечественные и зарубежные исследователи на протяжении последних нескольких лет пытаются выяснить причины наиболее активного использования соцсетей как отдельными преступниками, так и целыми преступными сообществами. По мнению специалиста в области уголовного права А.В. Манойло, это связано со следующими условиями:

- Несовершеннолетние пользователи в силу физиологических возрастных особенностей в условиях использования интернет-ресурса не обладают критическим мышлением, их бдительность снижена, что делает их потенциальными жертвами.
- Утрата способности избирательности у человека в части его окружения и ближайшего круга общения размывается в условиях мнимого ощущения неприкосновенности в виртуальном пространстве.

- На данном этапе развития эволюции человека исключается возможность восприятия в качестве объекта опасности картинки. Именно ей (так называемым аватаром) представлена в соцсети личность любого пользователя. На уровне подсознания в качестве угрозы может распознаваться лишь физический объект, поэтому преступник без труда втирается в доверие.

- Чёткие границы привлечения к ответственности в виртуальном пространстве также размываются вследствие сложности раскрытия преступления [2].

По нашему мнению, исследователем А.В. Манойло не было указано ещё одно актуальное на сегодняшний день условие развития преступности в соцсетях – минимизация личного взаимодействия граждан в условиях карантина из-за опасной болезни COVID-19. Изоляция в домашних условиях напрямую повлияла на переход весомой части несовершеннолетних в онлайн-режим. В частности, компания GlobalWebIndex при поддержке команды соцсети «VK Coffe» произвела опрос 12 тысяч граждан из 13 стран и установила, что с 2020 года численность активных пользователей соцсетей пополнилась на 45%.

Статистические данные Следственного комитета Российской Федерации свидетельствуют о том, что смена образа жизни взрослых и детей в условиях карантина повлияла на показатели, связанные с преступностью в Интернете. В частности, в 2020 году в Интернете было совершено 510 369 преступлений, что превышает аналогичные показатели 2019 г. более чем на 73%. Среди них 677 фактов незаконной организации и проведения азартных игр, 589 случаев распространения порнографических материалов с изображением несовершеннолетних, более 2700 хищений чужого имущества, иные тяжкие преступления, связанные с незаконным оборотом наркотиков и экстремистскими проявлениями, в том числе совершаемые детьми и подростками [6].

«Постоянное сидение дома закономерно приводит к увеличению времени, проводимого несовершеннолетними в интернете. Поэтому повысились риски совершения против детей преступлений с использованием информационно-телекоммуникационных сетей» – указала зампредседателя Следственного комитета РФ Е.Е. Леоненко [9].

Соответственно, данное условие стало причиной роста преступлений, совершаемых посредством использования социальных сетей.

В.С. Соловьёв внёс предложение введения статистических данных преступлений, совершаемых с использованием соцсетей. Несмотря на то, что подобные преступления имеют латентный характер, отечественному специалисту удалось осуществить собственную систематизацию: незаконный оборот наркотиков (24,5%); посягательства на частную собственность (18,4%); преступления экстремистского и террористического характера (10,9%); распространение порнографии (10,3%); преступления против конституционных прав человека (9,1%); преступления в сфере компьютерной информации (7,9%); преступления против жизни и здоровья (5,4%); иные общественно опасные деяния [4].

Причём 81% из вышеперечисленных преступлений совершались во «ВКонтакте». Таким образом, несовершеннолетние, составляющие весомую часть пользователей социальной сети «ВКонтакте», наиболее часто становятся жертвами педофилов, администраторов групп смерти, занимающихся пропагандой самоубийства, мошенников [1].

В первую очередь, хотелось бы отметить, что государственные органы, в частности, органы внутренних дел осуществляют активный мониторинг недоброкачественного контента в виртуальной сети с целью последующей его ликвидации и привлечения к ответственности виновных.

Наиболее свежая статистика Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций демонстрирует, что в период с 2012 по 2018 гг., благодаря оперативным действиям внесены в реестр и заблокированы более 350 тыс. онлайн-ресурсов, на которых была размещена запрещённая информация. В частности, более чем на 92 тыс. подобных ресурсов осуществлялся незаконный оборот наркотиков (из них удалено 81 660 страниц, к 11 088 страницам доступ ограничен). На основании данного опыта был сделан вывод, во-первых, о беспрецедентном омоложении наркобизнеса, ведь средний возраст сбытчика составляет 19 лет, во-вторых, о значительном увеличении случаев вовлечения несовершеннолетних пользователей в сбыт наркотиков в онлайн-режиме именно через социальные сети и мессенджеры [7].

В рамках проделанной работы было заблокировано более 65 тыс. ресурсов, на которых распространялась детская порнография. Причём с июня 2017 г. по 2018 г. было обнаружено более 26 тыс. противозаконных материалов по признакам преступлений, предусмотренных пунктом «г» ч. 2 ст. 242.1 УК РФ. По признакам данного состава преступления было осуждено всего 189 человек.

Более чем на 39 тыс. страницах была размещена информация с призывом к самоубийству, 14 тыс. страниц с суицидальным контентом были внесены в специализированный Единый реестр запрещенной к распространению в России информации с начала 2020 года. Так называемые группы смерти – наиболее опасные страницы, активно размещаемые в социальных сетях в 2016-2017 гг.

В качестве примера можно привести игру «Синий Кит». По хештегу #синийкит более 800 пользователей социальных сетей в 2017 г. ждали, что им напишет куратор – мошенник, который раздавал каждому желающему задания (по одному в течение 50 дней) – от самого простого (например, забраться на крышу) до самого сложного (к примеру, сделать разрез на коже). На пятидесятый день у каждого подростка, вовлечённого в игру, задание было одинаковое – покончить жизнь самоубийством. Игра «Синий Кит» и подобные ей игры («Тихий дом», «Море Китов», «Разбуди меня в 4:20» и другие) спровоцировали смерть сотен школьников России.

Согласно статистике Следственного комитета РФ, за последние три года суицид совершили 2 205 детей и подростков. При этом отмечается, что попытки суицида многократно превышают число реальных самоубийств, а для половины из подростков такие попытки являлись неоднократными, а систематическими [9]. Кроме того, весомым фактором криминализации несовершеннолетних являются группы, пропагандирующие криминальный образ жизни. В качестве примера можно привести группы АУЕ («Арестантский уклад един») в соцсетях, состоящие из неформальных банд детей и подростков, идеализирующих и романтизирующих жизнь преступников. Система норм и ценностей, пропагандируемых в подобных сообществах, схожа с криминальной идеологией и подобной линией поведения. С 2016 г. по сей день детьми и подростками совершаются преступления с характерными криками «АУЕ».

Так, 24 августа 2018 г. компания из 15 подростков в течение двух часов ходила и избивала прохожих на улицах Санкт-Петербурга. Жертвами банды стали 16 чел. В результате совершения преступления было возбуждено 2 уголовных дела по статьям «Побои» и «Умышленное причинение средней тяжести вреда здоровью».

Мониторинг и ликвидация сообществ «АУЕ» в социальных сетях началось ещё в 2017 г. По утверждению представителя Генеральной прокуратуры России, в 2017-2018 гг. при поддержке региональных судов было заблокировано более 7 тыс. преступных сообществ.

17 августа 2020 г. Верховный суд РФ постановил признать международное общественное движение АУЕ экстремистской организацией; с 2018 года стали ужесточаться наказания за склонение детей и подростков к суициду; были заблокированы соответствующие группы во «ВКонтакте» и «Одноклассниках» [8].

Кроме того, перспективным, по нашему мнению, является изменение ст. 128.1 УК РФ, а именно – ужесточение уголовной ответственности за клевету и оскорбления, которые также являются популярным составом преступлений в соцсетях. Так, с 10 января 2021 г. в ст. 128.1 были добавлены дополнительные квалифицирующие составы, а также значительно увеличен штраф за совершение преступления (за клевету – 1 000 000 руб., за ложное обвинение в преступлении против половой неприкосновенности – до 5 000 000 руб.) [8].

Также важные изменения коснулись ст. 230 УК РФ – Склонение к употреблению наркотических средств, психотропных веществ или их аналогов. В частности, с 7 марта 2021 г. уже действуют новые квалифицирующие обстоятельства для данного состава преступления –использование Интернета для совершения преступления.

Кроме того, хотелось бы остановиться на рассмотрении новых деяний, которые стали популярны в соцсетях с 2019-2020 г. Именно по этой причине данные деяния до сих пор не вошли ни в один состав преступлений, однако каждое из них несёт угрозу для развития детей и подростков.

- «Зумбобинг». Во время самоизоляции наиболее популярным приложением, предназначенным для дистанционного обучения, стал Zoom, позволяющий создать онлайн-платформу для взаимодействия неограниченного круга лиц по аудио- и видеосвязи. Отсутствие жестких мер безопасности в этом сервисе привело к появлению нового вида хулиганства, получившего название «зумбомбинг», когда пользователь подключается к чужой конференции и загружает на всеобщее обозрение порноролики или другой контент, который может быть неприемлем для определенных обучающихся.

Одно из первых нападений было реализовано на одном из занятий школ Норвегии. Организаторы видеоконференцсвязи вынуждены были остановить онлайн-занятие после того, как в чате класса появился голый человек – неизвестный мужчина, подключившись к конференции, адрес которой он подобрал вручную, разделся на глазах у нескольких несовершеннолетних детей. Важно отметить, что в последнее время зафиксировано несколько подобных случаев, когда взрослые люди намеренно ищут видеоконференции со школьниками, которые вынуждены обучаться удаленно из-за коронавируса.

При этом отсутствие в диспозиции ст. 213 УК РФ «Хулиганство» оснований для привлечения данных нарушителей порядка к уголовной ответственности,

способствуют их полной безнаказанности (до сегодняшнего дня ни один субъект не был привлечён к ответственности).

- «Секстинг». Наиболее популярное в социальных сетях действие, связанное с рассылкой чужих фотографий интимного характера. Исследование социальных сетей, в частности, «ВКонтакте» позволило выявить более 100 тыс. групп с целевой аудиторией численностью до 10 тыс. человек, в которых регулярно осуществляется рассылка подобных фотографий.

Отсутствие законодательного закрепления данного деяния, а также факт существования и регулярного обновления вышеуказанных сообществ, позволяют сделать вывод о полной безнаказанности виновных.

- «Грумминг». Целенаправленное установление дружеских отношений с ребёнком с целью последующего вступления с ним в половой контакт – новый вид насилия над несовершеннолетними. Особая опасность действий нарушителя кроется в том, что своевременно предупредить или пресечь последствия невозможно. Сущность деяния заключается в следующем: мужчины (как показывает практика, зачастую их возраст превышает тридцать лет) создают в социальной сети фэйковую страницу ребёнка – ровесника будущей жертвы и завязывают дружеский диалог с несовершеннолетним, повествуя выдуманные истории из жизни, поддерживая его. Особое психологическое давление, оказываемое на ребёнка, зачастую является поводом для добровольного выполнения «просьб» виртуального знакомого.

Безусловно, каждое из представленных нами нарушений представляет особую опасность для физического и психологического развития несовершеннолетних. Однако факт отсутствия диспозиций соответствующих статей препятствует оперативно-розыскным подразделениям предупредить и пресечь эти преступления для последующего возбуждения административных или уголовных дел. По нашему мнению, устранение таких пробелов в законодательстве является необходимостью в настоящее время.

В первую очередь отметим, что в уголовном законодательстве США уже существует такой состав преступления как «Зумбобинг». По нашему мнению, следует внедрить данный состав преступления и в Российское законодательство в качестве квалифицирующего обстоятельства для ст. 213 УК РФ «Хулиганство».

Далее отметим, что нам представляется целесообразным ввести новый состав правонарушения в Кодексе Российской Федерации об административных правонарушениях от 30.12.2001 г. № 195-ФЗ – «Секстинг».

Наконец, «Грумминг», по нашему мнению, должен стать квалифицирующим признаком для ст. 134 УК РФ «Половое сношение и иные действия сексуального характера с лицом, не достигшим шестнадцатилетнего возраста».

Таким образом, современная архитектура общедоступности, открытости, востребованности и децентрализованности социальных сетей делает их легким орудием для совершения преступлений как несовершеннолетними, так и в отношении них.

Список литературы:

1. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (с учетом последних изменений) // Справ.-правовая система [Электронный ресурс]. URL: <http://www.consultant.ru/> (дата обращения: 20.08.2022).
2. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (последняя редакция) // Справ.-правовая система [Электронный ресурс]. URL: <http://www.consultant.ru/> (дата об-

ращения: 20.08.2022).

3. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон от 06.07.2016 № 374-ФЗ // Справ.-правовая система [Электронный ресурс]. URL: <http://www.consultant.ru/> (дата обращения: 20.08.2022).

4. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон от 06.07.2016 № 375-ФЗ // Справ.-правовая система [Электронный ресурс]. URL: <http://www.consultant.ru/> (дата обращения: 20.08.2022).

5. Симидзу Рё. Искусственный интеллект в Японии: глубокое обучение и текущая ситуация [Электронный ресурс]. URL: <https://www.nippon.com/ru/currents/d00307/> (дата обращения: 14.08.2022).

6. Озеров И.Н. Осуществление оперативно-разыскной деятельности в особых условиях // Расследование преступлений: проблемы и пути их решения. 2021. № 2 (32). С. 109–112.

7. Зоз В.А., Шроль А.Р. Использование технологий искусственного интеллекта в правоохранительных органах // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2021. Т. 7. № 2. С. 191–194.

Lagutochkin A. V. The essence, formation and prospects of using neural network technologies in operational investigative activities // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2022. – Т. 8 (74). № 4. – P. 354-365.

The article reveals the question of the legal genesis of the problems associated with juvenile delinquency, The article reveals the formation and prospects of use of neural network technologies (artificial intelligence) by internal affairs units, carrying out operational and investigative activities.

The use of neural network technology is one of the most important prerequisites for the structural construction of state security, where artificial intelligence acquires the status of a tool in achieving the primary goals of law enforcement agencies.

Having chosen the goal to take its rightful place among the leading countries of the world in the development of the information society, our country is actively developing its own information and telecommunications infrastructure. It can be stated that the state has moved from declaring intentions in the mentioned sphere to concrete actions, and notable results have already been achieved on this way.

The use of artificial intelligence in law enforcement determines the innovative approaches to detection, prevention, suppression and solving of crimes in the Russian Federation.

Keywords: artificial intelligence, neural networks, operational-search activities, operational-search activities, records.

Spisok literatury:

1. Ob operativno-rozysknoj deyatel'nosti: Federal'nyj zakon ot 12.08.1995 № 144-FZ (s uchetom poslednih izmenenij) // Sprav.-pravovaya sistema [Elektronnyj resurs]. URL: <http://www.consultant.ru/> (data obrashcheniya: 20.08.2022).

2. Federal'nyj zakon «O svyazi» ot 07.07.2003 № 126-FZ (poslednyaya redakciya) // Sprav.-pravovaya sistema [Elektronnyj resurs]. URL: <http://www.consultant.ru/> (data obrashcheniya: 20.08.2022).

3. O vnesenii izmenenij v Federal'nyj zakon «O protivodejstvii terrorizmu» i otdel'nye zakonodatel'nye akty Rossijskoj Federacii v chasti ustanovleniya dopolnitel'nyh mer protivodejstviya terrorizmu i obespecheniya obshchestvennoj bezopasnosti: Federal'nyj zakon ot 06.07.2016 № 374-FZ // Sprav.-pravovaya sistema [Elektronnyj resurs]. URL: <http://www.consultant.ru/> (data obrashcheniya: 20.08.2022).

4. O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i Ugolovno-processual'nyj kodeks Rossijskoj Federacii v chasti ustanovleniya dopolnitel'nyh mer protivodejstviya terrorizmu i obespecheniya obshchestvennoj bezopasnosti: Federal'nyj zakon ot 06.07.2016 № 375-FZ // Sprav.-pravovaya sistema [Elektronnyj resurs]. URL: <http://www.consultant.ru/> (data obrashcheniya: 20.08.2022).

5. Simidzu Ryo. Iskusstvennyj intellekt v Yaponii: glubokoe obuchenie i tekushchaya situaciya [Elektronnyj resurs]. URL: <https://www.nippon.com/ru/currents/d00307/> (data obrashcheniya: 14.08.2022).

6. Ozerov I.N. Osushchestvlenie operativno-rozysknoj deyatel'nosti v osobyh usloviyah // Rassledovanie prestuplenij: problemy i puti ih resheniya. 2021. № 2 (32). S. 109–112.