DOI 10.36622/1682-7813.2025.28.2.004
УДК 343.211.5

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В.А. Минаев, К.М. Бондарь

Обсуждаются существующие подходы к решению задач правоохранительных органов по противодействию киберпреступности на основе технологий искусственного интеллекта (ИИ). При этом рассматриваются и факторы применения ИИ со стороны криминальной среды. Особое внимание придается атакам со стороны кибермошенников с помощью методов искусственного интеллекта и социальной инженерии. Производится анализ состояния и динамики киберпреступности по статистическим данным. Делается акцент на киберзащите граждан страны как ключевой задаче подразделений МВД России. Показываются пути активного применения технологий ИИ для решения задач кибербезопасности: совершенствование нормативного правового обеспечения, психоэмоциональная поддержка граждан, противодействие новым киберугрозам населению и организациям. Раскрывается тема цифровых следов как основы оперативно-розыскных мероприятий в Сети. Приводятся примеры использования ИИ при раскрытии и расследовании серийных преступлений, профилактике преступлений. Делается вывод о перспективности применения технологий больших данных, имитационного моделирования и нейронных сетей при организации противодействия киберпреступлениям.

Ключевые слова: киберпреступность, кибербезопасность, социальная инженерия, правоохранительные органы, противодействие, профилактика, искусственный интеллект, нейронная сеть.

Введение

Научные достижения различного уровня всегда создавали условия для возникновения и дальнейшего формирования как позитивных, так и негативных тенденций в историческом развитии общества. Происходящая сегодня четвертая промышленная революция предоставляет человечеству спектр принципиальных новых возможностей опять измениться. Среди них ключевой выступает искусственный интеллект (ИИ) и приложения интеллектуальных технологий.

В области их положительных аспектов нашли реальное применение и продолжают развиваться интеллектуальные технологии противодействия преступным проявлениям, в том числе – в сфере киберпреступлений. Но все больше проявляется и обратная сторона позитивных процессов. Она связана с тем, что криминальные сообщества сумели найти и для себя концептуальный смысл и практические приложения технологических достижений ИИ в процессах разработки, обеспечения, реализации и сокрытия самих преступных кибердеяний и их конкретных видов.

По оценке Главного информационно-аналитического центра МВД России, в течение последних 10 лет число киберпреступлений возросло на два порядка.

Современная киберпреступность

Сегодня в общей структуре преступности в России доля преступлений, совершенных с использованием информационно-телекоммуникационных технологий, уже превысила одну треть. Эта тенденция, отражает все более повышенный интерес криминалитета к использованию достижений информационной науки и цифровой техники и, в первую очередь, технологий ИИ, в своей преступной деятельности.

Так, в исследовании [1], посвященном состоянию кибербезопасности в 2024 г., среди основных видов атак в арсенале мошенников выделены технологические новинки с помощью методов искусственного интеллекта и социальной инженерии, как занимающие первое место в общем перечне киберпреступлений.

Существенная активизация российских кибермошенников в прошедшем году привела к хищениям у граждан страны около 250 млрд рублей.

По данным центра мониторинга *RED Security SOC* количество атак на российские компании возросло в 2,5 раза, мошенники освоили генеративный искусственный интеллект для создания поддельных сайтов, писем, аудио и видеозвонков. Стал чрезвычайно опасным преступный тренд прошедшего и текущего года, связанный с психологическими атаками на население: аферисты, манипулируя эмоциями людей, принуждали жертв переводить деньги на «безопасные счета».

Редакция *Hi-Tech Mail*, эксперты МТС *Future Crew* и *Kaspersky GReAT*, объясняя особенности преступного использования ряда технологии, созданных для пользы людей, но переориентированных против них же, подчеркнули опасности современных нейросетей и киберугроз текущего 2025 г.

Авторы обзора [1] подчеркивают, что количество киберинцидентов в прошлом году по сравнению с 2023 г. увеличилось на 39 %. В их числе – онлайн-мошенничество, фишинг, заражение компьютерных устройств вредоносным программным обеспечением и другие противоправные действия, что привело к охвату различного рода киберугрозами около 57% российских пользователей.

Всё это стало возможным во многом в связи с доступностью интеллектуальных программных инструментов, а также с массовым стремлением киберпреступников использовать технологии нейронных сетей. Это в полной мере относится к области так называемого генеративного ИИ. Порядка 40% фишинговых сообщений по электронной почте генерируется именно им.

С его помощью осуществляются противоправные процедуры по созданию контентов фишинговых веб-сайтов, страниц ведущих соцсетей, государственных структур, банков, фейковых «брендовых» магазинов, где предлагаются фейковые акции и скидки на товары.

Кроме расширения компьютерного онлайн-мошенничества, все больший размах приобретает телефонное мошенничество с использованием ИИ – в основном, на базе нейронных сетей генерация поддельных аудио- и видеоматериалов в «реальном времени».

Это позволяет более целенаправленно атаковать эмоциональную сферу потенциальных жертв, притуплять их бдительность. Например, инсценировать сообщения от собственных руководителей, сотрудников правоохранительных структур; о попаданиях родственников в серьезные катастрофы; о больших проблемах по долгам; о неожиданных выигрышах; об оказании социальных или медицинских услугах со значительными скидками и т. д.

Человек как ключевой объект киберзащиты

Жесткая оценка происходящих негативных явлений в информационной сфере и необходимость осуществления неотложных мер по эффективному противодействию криминалитету прозвучала на весенней 2025 года Коллегии МВД России.

В выступлениях на ней Президента Российской Федерации В.В. Путина и Министра внутренних дел В.А. Колокольцева отмечен недопустимый рост кибермошенничества и размеров ущерба населения страны от данного преступного промысла, а сам факт его стремительного роста назван угрозой национальной безопасности [2].

Характеризуя работу по противодействию киберпреступлениям со стороны правоохранительных структур, сосредоточим основное внимание на возможностях искусственного интеллекта в эффективном обеспечении этой деятельности.

Исходя из этого, при создании киберзащиты объектов, требуется внедрить интеллектуальные технологические решения для минимизация возможного ущерба со следующим функционалом:

– превентивное влияние, заставляющее злоумышленника оценить силу специального противодействия и, возможно, отказаться от преступного замысла;

– создание условий для пользователя при эксплуатации персональных гаджетов, существенно снижающих психологическое воздействие со стороны кибермошенников,

сдерживающих их негативный напор, тормозящих механизмы критического восприятия ситуации психологического давления. На эти психологические реакции как раз и рассчитывают кибермошенники, – пытаясь дестабилизировать нормальное состояние своей жертвы. Именно на этой основе:

– организуется и осуществляется преступное воздействие на атакуемое лицо с целью изъятия у него денежных средств в физическом или электронном формате;

– обеспечиваются условия для раскрытия и расследования реально произошедшего или незавершенного преступления (также требующего уголовно-правовой оценки и, возможно, являющегося уголовно наказуемым, то есть влекущим проведение комплекса оперативно-розыскных и следственно-процессуальных мероприятий).

Исходя из приведенных рассуждений, видятся несколько путей активного применения технологий ИИ для решения задач кибербезопасности применительно к деятельности правоохранительных органов.

1. Нормативно-правовое обеспечение

Недавно принят новый федеральный закон [1], регламентирующий современные виды киберпреступлений, нашедших распространение в стране.

Рассмотрим некоторые предложения, указанные в этом нормативно-правовом документе. Их реальное воплощение предполагается на базе создающейся в стране государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий (ИКТ), содержащей следующий функционал:

– через технологические возможности сервиса «Госуслуг» пользователю стал доступен вариант установки самозапрета на дистанционное оформление сим-карт, исключая таким образом данную опцию со стороны злоумышленников;

– российские пользователи через операторов услуг связи могут установить самозапрет на международные звонки, спам- и массовые обзвоны, СМС-рассылки;

– при приеме звонков (вызовов) в обязательном порядке вводится маркировка вызывающей организации;

– автоматизирована процедура исключения сообщений пользователю от «Госуслуг» (включая код подтверждения);

– российские пользователи смогут использовать биометрию при получении микрозаймов;

– в случае отказа пользователя от какого-то номера телефона, он автоматически удаляется из личного кабинета «Госуслуг» и связанных с ним банковских приложений;

– госорганам, банкам, операторам связи и цифровым платформам запрещается использовать зарубежные мессенджеры для общения с клиентами. Запрет также распространяется и на владельцев агрегаторов товаров и услуг, сайтов и сервисов, которые ежедневно посещают более полумиллиона пользователей;

– автоматический контроль проведения операций в банкоматах будет способен прекращать общение с текущим пользователем в случае фиксации подозрительных действий;

– для банков вводится обязательство проведения мероприятий по антифроду не только на онлайн-платежи, но и применительно к банкоматам;

– банкам вменяется проверка признаков выдачи денег в банкомате без согласия клиента. В этом случае на 48 часов ограничивается выдача наличных.

Специалисты по кибербезопасности напоминают, что, наряду с новыми решениями правового характера, необходимо продолжать использовать уже оправдавший себя эффективный опыт.

А именно, исключить обращение к файлам из сомнительных источников, подозрительным ссылкам; программные приложения и платформы эксплуатировать с условием официального регулярного обновления; сделать обязательными процедуры защиты своих аккаунтов на основе сложных и уникальных паролей, многофакторной аутентификации, использования надежных антивирусных решений.

2. Психоэмоциональная поддержка граждан

Противоправные деяния в сфере киберпреступности, как правило, связаны с эмоциональной дестабилизацией жертвы кибернападения, запуском механизма психологического расстройства.

Эффективность атаки базируется на информации, рассчитанной на проявление разных эмоций, например, возникновение испуга, страха, полной прострации, мотивов быстрого обогащения.

В любом случае возникновение эмоционального стресса приводит к непониманию возникшей ситуации, осознанию наказуемой безответственности, наступления нежелательных последствий (личных, родственных, общественных и иных).

Задача инструментария ИИ – не допустить длительного эмоционального воздействия на потенциальную жертву. Смысл временн***о***й задержки состоит в том, чтобы атакуемый человек не успел «запустить» определенные психологические механизмы и не дать мозгу соответствующей мотивации для выработки эмоциональных реакций на происходящее воздействие, которое, чаще всего, выражается как фейковые «оригинальные» обстоятельства, излагаемые кибермошенниками.

В этих целях крупными финансовыми организациями (например, банками СБЕР, ВТБ) создаются интеллектуальные программные продукты под условным наименованием «защитники».

Необходимо отметить, что кроме непосредственного распознавания спуфинга, который фактически является кибератакой на конкретного пользователя сотовой сети или иного гаджета, задача технологий ИИ не должна ограничиваться данной процедурой.

Важной и приоритетной следует считать разработку возможностей рассматриваемого инструментария, позволяющих обеспечить мероприятия по оперативной фиксации цифровых следов проводимого воздействия.

Они должны стать источником криминалистически значимой информации, отражать признаки «серийности» кибератак, способствовать деанонимизации, то есть определению истинных характеристик исполнителей для выявления подозреваемого в совершении преступления, а при наличии комплекса доказательств - предъявления уголовного обвинения.

3. Противодействие новым киберугрозам населению

Криминальное направление, быстро прогрессирующее в последнее время, связано с поиском «слабых мест» программных продуктов. При этом технологии ИИ стали эффективным инструментом поддержки преступных замыслов.

Злоумышленниками фактически проводится подобие научного исследования, моделирования сценариев неправомерного использования найденных уязвимостей, а также социальных, экономических и иных сфер внедрения и распространения результатов своеобразных «криминальных НИР».

Таким образом, каждая разновидность программных недостатков, технологических или организационных недоработок, происхождения искусственного или случайного обнаруживается не только сотрудниками правоохранительных органов, но и весьма квалифицированными участниками преступных групп.

В противоправной среде именно обращение к ИИ позволяет проводить своеобразные исследования по моделированию возможного негативного развития конкретных ситуаций, вызванного влиянием параметров выявленной «слабости» программного обеспечения.

Высказанные соображения приводят к выводу, что необходимо опережающими темпами наращивать аналогичные процедуры и специализированным правоохранительным структурам, ответственным за противодействие киберпреступности в стране. Нужно опережать криминалитет и в специальной подготовке в области цифровых технологий, математических моделей и методов.

Сегодня много сделано и делается в этом направлении. Однако практика показывает, что такой вывод оправдан. Следует реализовать, как принято говорить, дополнительные опции интеллектуального превентивного инструментария, включая технологии больших данных и

имитационного моделирования, а также сформировать эффективные методики по профилактике новых киберугрозугроз для индивидуальных пользователей – обычных граждан, наиболее часто подвергающихся кибермошенничеству и являющихся для правоохранительных структур категориями высшего приоритета, требующими усиления их киберзащиты.

Цифровые следы – основа оперативно-розыскных мероприятий в Сети

Данная тема раскрыта в целом ряде научных источников и результатов исследований. Их общий итог довольно единодушен, состоя в необходимости повышения уровня оперативно-розыскной работы за счет поиска и систематизации цифровых следов лиц и объектов оперативного интереса в информационной сфере. Существенное повышение эффективности этих процессов базируется на активном внедрении и применении технологий ИИ.

Не ставя задачу полного системного отражения специфики и особенностей создания таких технологий, а предполагая формирование понятийного аппарата в этой области, обратимся к одной из современных работ [3], которая, по нашему мнению, как раз и дает необходимый срез раскрытия рассматриваемых аспектов.

В работе автор делает попытку оценить оперативно-розыскной аспект, применимость *интеллектуальной поддержки* задач поиска ориентирующих и доказательственных сведений о преступлениях, *совершаемых с использованием ИКТ,* в правоохранительной деятельности при обращении к Интернет как средству распространения информации.

В работе, прежде всего, выражается целесообразность создания в системе МВД России единой базы данных по систематизации сведений и результатов оперативно-розыскных мероприятий (ОРМ). Речь идет об ОРМ при организации противодействия преступлениям данного вида (круг лиц оперативного интереса; способы совершения; типы используемого программного обеспечения; виды пострадавших банковских и иных структур, юридических или физических лиц и т. д.).

Обычным подходом российских пользователей Интернет являются информационные операции в «своем» виртуальном пространстве, то есть в доменной зоне *.RU*, которая находится под контролем правоохранительных органов страны.

Но применение известных технологий позволяет переходить в информационные поля других государств (в случае, когда подозреваемый в мошенничестве является иностранным гражданином), что создает существенные проблемы для получения требуемых оперативно-розыскных сведений.

Приведенные и иные обстоятельства противодействия киберпреступности делают актуальной задачу разработки специальных интеллектуальных программных продуктов. Их целевая направленность должна выражаться в способности минимизировать противоправные действия со стороны граждан иностранных государств, а также участников российского криминалитета, которые для совершения преступлений подобного рода обращаются к возможностям опций и технологий зарубежных транзитных доменов или сайтов.

Показательным примером требуемых разработок и их практического внедрения и применения является система с интеллектуальной поддержкой, остроумно названная «великим китайским файрволом» и развернутая в интересах правоохранительных структур КНР [4].

Аналогичные с А. Поздняковым [1] позиции поддерживают и другие авторы, среди которых отметим работу [5], в которой А. Бабушкин определяет возможности внедрения модели системы оперативно-розыскного контроля за лицами, склонными к совершению преступлений. Для этого рассматриваются правовые основы системы, ее организационно-тактические формы, информационно-аналитическое обеспечение, основанное на применении ИКТ, в том числе базирующихся на ИИ.

Противодействие серийным преступлениям

Преступления данного вида считаются одними из самых сложных в раскрытии и расследовании, в том числе и в области

киберпреступности. Они требуют высокопрофессиональных подходов и умений, специализированной тактики в процессах поиска, сбора, информационного обоснования выдвигаемых версий.

Эффективную помощь в этом могут оказать подходы и методы использования технологий ИИ.

Особенности научной проработки и организации внедрения в практику подобного инструментария можно проследить в работе коллектива авторов [6].

В ней ставилась задача применения одного из методов ИИ – машинного обучения – и последующего анализа данных в целях выявления признаков серийности определенных категорий преступлений.

Основу эмпирической базы работы составили систематизированные обращения к совокупности данных по раскрытым и оконченным расследованиями серийных преступлений против личности. В частности, анализировались 370 эпизодов по расследованиям, подследственными в которых выступали печально известные в прошлом фигуранты (например, Чикатило, Ряховский, Табардин, Миргород). В качестве характеристик, отражавших особенности преступных эпизодов, оценивались 76 специфических реквизитов – тип преступления, наличие сопутствующих деяний, место совершения, время и т. д.

Применение технологий ИИ в решении задачи заключалась в разработке и апробации специального интеллектуального программного обеспечения. Созданный алгоритм тестировался на возможность выделения отдельных эпизодов в серии.

Общий результат тестовой эксплуатации составил 72,5% соответствия модельных выводов материалам расследований реальных преступлений против личности. Так, для серии под фамилией серийного убийцы «Миргород» следователями доказано 16 эпизодов, а модель ИИ сформировала серию из 14 эпизодов (87,5%). Карта систематизации эпизодов преступлений искусственным интеллектом приведена на рис. 1.

Успешность работы ИИ указала на перспективность подобных приложений. В то же время, тщательный анализ выявил и некоторые недостатки при отнесении отдельных информационных элементов к предполагаемой серии.

По мнению авторов, они связаны, прежде всего, с неполнотой заполнения исходных учетных и регистрационных карт в базах данных. Ими же отмечается недостаток, связанный с влиянием некорректного внесения сведений и отсутствием надежного программного контроля такого внесения.

Кроме того, сказывался известный эффект при формировании баз данных – *терминологические различия в описании одних и тех же объектов*.

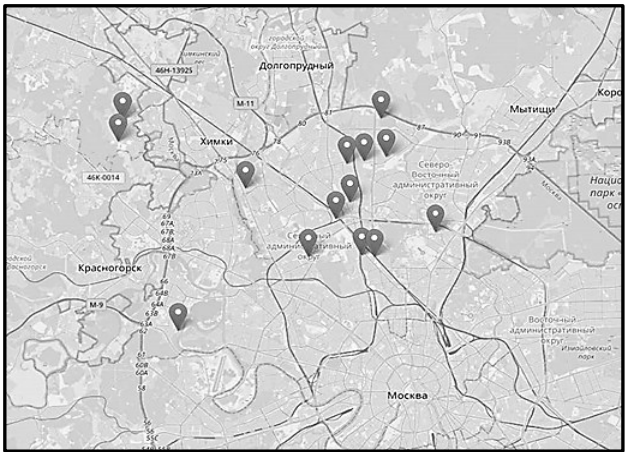

Рис. 1. Карта выявления ИИ эпизодов серии убийств «Миргород» [5]

В целом же применение ИИ перспективно и по другим направлениям интеллектуальной поддержки оперативно-служебных задач правоохранительных органов, в частности – при противодействии киберпреступлениям.

Этот тезис убедительно подкрепляется активным продвижением технологий ИИ в системе информационно-аналитического обеспечения МВД России – ИСОД. Элементы указанных технологий имеются в автоматизированных системах «Карта криминогенности», «Следопыт-М», аппаратно-программном комплексе «Безопасный город», специальном программном обеспечении систем «Паутина», «Сфера» и в ряде других.

Такого рода системы дают пользователям возможность для проведения глубокого анализа данных на предмет выявления оперативно значимой информации,

обоснования розыскных и следственных версий и сбора доказательств и фактов (из открытых и закрытых источников) без специальных знаний в программировании и эксплуатации ИКТ.

Подобного рода система *Zero Trust* (КНР, эксплуатируется с 2016 г.) имеет доступ к 150 государственным, финансово-кредитным базам данных с информацией о деловой и социальной жизни госслужащих, используя *модель безопасности с нулевым доверием – ZTA*. Концептуально в отмеченной системе реализуется принцип «никогда не доверять, всегда проверять».

Профилактика киберпреступлений

Информационное обеспечение предупреждения киберпреступлений, в частности, связано с созданием и развитием теории экспертной профилактики, представленной в работах В. Федоровича, см. например, [7]. Базовые позиции указанных работ выражаются в двух направлениям.

Первое направление связано с необходимостью криминалистической поддержки следственных действий и судебных экспертиз на основе технологий больших данных и ИИ, аналитической разведки *OSINT*. Как правило, при этом не идет речь о применении возможностей разведки *HUMINT* (*HUMan INTelligence*), относимой к технологиям социальной инженерии применительно к «разведке по людям» посредством специальной агентуры.

Второе направление ориентировано на выявление системных закономерностей в социальных медиа, криминалистических учетах, результатах аналитических разведывательных мероприятий *OSINT*. Подобный комплекс также базируется на технологиях ИИ, и нацелен на установление некоторых закономерностей, интересных в оперативно-разведывательном или доказательственном плане, относящихся к отождествляющим или характеризующим признакам, информационным связям между различными хранилищами данных и форматами хранения (тексты, изображения).

Совокупность полученных материалов может служить для выработки типовых рекомендаций по способам совершения правонарушений или преступлений, оригинальным или повторяющимся особенностям их проявлений. Это обеспечивает меры профилактического воздействия при ожидании аналогичных происшествий в целях быстрого реагирования на них и снижения б***о***льшего физического и морального ущерба.

В дополнение охарактеризуем некоторые особенности современного понимания указанного направления, обратившись к работе О. Русецкого [8], где освещены основы системы профилактики преступлений в кибернетическом пространстве.

Данный вид преступности, характерный для киберпространства, поддерживается: генерацией новых противоправных средств и способов; технической и технологической средой с потенциальными путями реализации преступных деяний; быстрыми и качественными изменениями общественного сознания, образа жизни населения.

Раскрывая последний аспект, важно отметить, что современные процессы модернизации социума значительно определяют детерминацию девиантного и криминального поведения, среди них:

– реализация достижений технологий информационного характера в детской среде. На основе быстрого и, как правило, увлекательного удовлетворения детей в потребности познания мира, гаджеты способны стать «другом», постоянным помощником. В криминологическом плане развивающаяся при этом серьезная привязанность несовершеннолетних к информационно-коммуникационной среде является основой проблем социализации, а затем, по мере погружения в противозаконный контент, возникает активное взаимодействие с противоправными проявлениями и их акторами в виртуальном пространстве;

– воздействие на сознание и мировоззрение населения посредством виртуализации. Искусственная реальность, особенно в детском и подростковом возрасте, на основе коммуникативного или игрового подхода способна на принципиально новом уровне обеспечить редукцию значимых элементов социальной действительности. В результате снижаются шансы адекватной оценки событий, мотивируется неуверенность

в будущем, фрустрация, возможно появление анархических настроений. Подобным образом сформированные личности могут неадекватно воспринимать реальное уголовное преследование, решения правоохранительной и судебной систем;

– формирование сетевой зависимости не отрицаются в исследованиях психологии, медицины, социологии, требуя ее внесения в перечень поведенческих зависимостей в качестве нового вида, порожденного интернет-средой и ИКТ. Такая зависимость способна создавать возможности для осуществления противоправных видов поведения, служить причиной снижения нормальных процессов социализации конкретных личностей;

– влияние сетевых и информационных технологий на возможности достижения деструктивных политических целей, организации и осуществления, в том числе – и киберпреступлений.

Кроме сказанного, в современном обществе стало критическим влияние и иных факторов, определяющих новые виды противоречий. Среди них – интенсивное освоение информационных технологий и низкий уровень компьютерной грамотности; дисгармония в тенденциях информационных технологий и технологического уровня их разработки в стране; отличия в темпах разработки, внедрения и освоения норм правового регулирования в сфере кибербезопасности; возникновение новых кредитно-финансовых отношений, появление изощренных мошеннических алгоритмов и схем посягательств на чужие активы и на этом фоне – чрезвычайно высокая виктимогенность населения.

Исходя из приведенных положений, укажем, что предупреждение преступности в киберпространстве должно быть направлено на выявление и устранение факторов, причин и условий криминального поведения среди тех, кто взаимодействует в виртуальном пространстве. Исследователи называют и другие особенности киберпреступлений, их прогнозирования на основе технологий ИИ, а затем – выработки подходов к их профилактике.

Так, В. Давыдов [9] занимается вопросами оценки использования ИИ криминалитетом в целях превентивной разработки сценариев развития криминальных событий, с одной стороны, и формирования требуемого комплекса методов и средств эффективного проведения расследования в данных обстоятельствах.

Статья Н. Старостенко [10] базируется на анализе способа мошеннических действий с использованием DeepFake-технологий и обрисовывает основы формирования прогностического подхода для поддержания следственной деятельности по хищениям, совершенным в сфере ИКТ.

В работе А. Суходолова и А. Бычковой [11] акцентируется внимание на опыте применения программных продуктов ИИ для профилактики преступности: прогнозная психометрика преступного сообщества – *COMPAS*; *Harm Assessment Risk Tool*; аналитический программный комплекс *CEG*; система прогнозирования преступлений *PredPol*; система *ePOOLICE*; программные продукты *Palantir*; российская система «Искусственный интеллект». В целях количественной оценки профилактической деятельности предлагается ряд индикаторов, раннего предупреждения преступности.

Работа А. Соколовой [12] отражает применение технологий ИИ в таком процессе как цифровизация судебно-баллистической экспертизы. Статья является примером исследования, направленного на обеспечение интеллектуальной поддержки экспертно-криминалистической деятельности. Подобного рода исследования в настоящее время активно развиваются в системе МВД России, являясь, перспективным направлением противодействия киберпреступности.

Обсуждение и выводы

При обсуждении современных решений задач правоохранительных органов по противодействию киберпреступности на основе технологий искусственного интеллекта (ИИ) необходимо рассматривать и факторы применения ИИ со стороны криминальной среды. Особое внимание следует придать атакам со стороны кибермошенников с помощью методов искусственного интеллекта и социальной инженерии. При этом основной акцент

делается на киберзащите граждан страны как ключевой задаче правоохранительных органов. Среди основных направлений активного применения технологий ИИ для достижения приемлемой степени кибербезопасности стоить выделить: современное нормативное правовое обеспечение, поддержку граждан в психоэмоциональном плане, укрепление системы защиты населения, объектов социальной и экономической инфраструктуры, организаций топливо-энергетического профиля, государственного управления от новых киберугроз. Важнейшим для правоохранительных органов является направление совершенствования их работы в области цифровых следов как основы оперативно-розыскных мероприятий в Сети. Ключевыми задачами при этом выступают использование ИИ при раскрытии и расследовании серийных и резонансных преступлений, профилактике преступлений, особенно в сфере кибермошенничества. Как показывает опыт, эффект применения ИИ многократно усиливается при включении в исследовательский процесс технологий больших данных, имитационного моделирования.

Заключение

В статье излагаются вопросы применения перспективных и эффективных технологий в раскрытии и расследовании киберпреступлений. Особый акцент делается на кибермошенничестве, как наиболее быстро развивающемся их виде. Суть предлагаемого подхода базируется на использовании достижений искусственного интеллекта, в частности на нейронных моделях. Показано, что данный подход уже успешно зарекомендовал себя при решении целого ряда оперативно-служебных задач органов внутренних дел. В дополнение раскрыты новые перспективные возможности интеллектуальной поддержки такого рода решений.

Список литературы

1. Бокова И., Галов Д., Котиков Н. Итоги кибербезопасности за 2024 год: атаки с помощью ИИ и манипуляция эмоциями. URL: https://hi-tech.mail.ru/review/121083-itogi-kiberbezopasnosti-za-2024-god/ (дата обращения 27.05.2025).

2. Расширенное заседание коллегии МВД. События. 2025. 5 марта. URL: http://www.kremlin.ru/events/president/news/76408 (дата обращения 27.05.2025).

3. Поздняков А.Н. Интернет и его функции в виртуальном пространстве: оперативно-розыскной аспект // Сетевое издание «Академическая мысль». 2024. № 4(29). С. 47-53.

4. Великий китайский файрвол: как Китай контролирует внутренний Интернет. URL: https://skillbox.ru/media/code/velikiy-kitayskiy-fayrvol-kak-kitay-kontroliruet-vnutrenniy-internet/ (дата обращения 27.05.2025).

5. Бабушкин А.А. Теоретико-правовая модель системы оперативно-розыскного контроля органов внутренних дел за лицами, склонными к совершению преступлений в условиях развития информационного общества // Философия права. 2024. № 3 (110). С. 95-101.

6. Владимиров В.Ю. Искусственный интеллект в борьбе с серийными преступлениями. Научная разработка в практику / В.Ю. Владимиров, И.А. Данилов, Н.Н. Ильин // Труды Академии управления МВД России. 2024. № 4 (72). С. 139-150.

7. Федорович В.Ю. К вопросу о технико-криминалистическом обеспечении предупреждения преступлений // Технико-криминалистическое обеспечение раскрытия и расследования преступлений [научное электронное издание]. М.: Московский университет МВД России имени В. Я. Кикотя. 2020. С. 11-13.

8. Русецкий О.В. Система профилактики преступлений в информационном пространстве // Криминалист. 2024. № 2 (47). С. 113-120.

9. Давыдов В.О. Преступность и искусственный интеллект: криминалистическое прогнозирование факторов благоприятствования // Философия права: научно-теоретический журнал. 2024. № 3. С. 109-115.

10. Старостенко Н.И. Криминалистическое прогнозирование хищений, совершаемых с использованием «DeepFake»-технологий // Вестник

Сибирского юридического института МВД России. 2023. № 2 (51). С. 187-192.

11. Суходолов А.П., Бычкова А.М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 753-766.

12. Соколова А.В. Цифровизация судебно-баллистической экспертизы: генезис и перспективы / Материалы междунар. науч.-практич. конф. «Криминалистика – наука без границ: традиции и новации». Санкт-Петербург, 2024. С. 520-523.

Московский университет МВД РФ им. В.Я. Кикотя
Moscow University of the Internal Affairs Ministry of Russia named after V.Ya. Kikot

Дальневосточный юридический институт МВД РФ им. И.Ф. Шилова
Far Eastern Law Institute of the Internal Affairs Ministry of Russia named after I.F. Shilov

Поступила в редакцию 30.05.25

Информация об авторах

Минаев Владимир Александрович – д-р техн. наук, профессор, профессор кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: m1va@yandex.ru

Бондарь Константин Михайлович – канд. техн. наук, профессор кафедры информационно-технического обеспечения Дальневосточного юридического института МВД РФ им. И.Ф. Шилова, e-mail: bondar_km@mail.ru

COUNTERING CYBERCRIME BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

V.A. Minaev, K.M. Bondar

The existing approaches to solving the tasks of law enforcement agencies in countering cybercrime based on artificial intelligence (AI) technologies are discussed. At the same time, the factors of the use of AI by the criminal environment are also considered. Special attention is paid to attacks by cybercriminals using artificial intelligence and social engineering methods. The analysis of the state and dynamics of cybercrime based on statistical data is carried out. The focus is on cyber protection of the country's citizens as a key task of the Russian Interior Ministry units. The article shows ways to actively use AI technologies to solve cybersecurity problems: improving regulatory support, Psycho-Emotional support for citizens, and countering new cyber threats to the public and organizations. The article reveals the topic of digital footprints as the basis of operational investigative measures on the Web. Examples of the use of AI in the detection and investigation of serial crimes and crime prevention are given. The conclusion is made about the prospects of using big data technologies, simulation modeling and neural networks in the organization of countering cybercrime.

Keywords: cybercrime, cybersecurity, social engineering, law enforcement agencies, counteraction, prevention, artificial intelligence, neural network.

Submitted 30.05.25

Information about the authors

Vladimir A. Minaev – Dr. Sc. (Technical), Professor, Professor of the Special Information Technologies Department, V. Ya. Kikot Moscow University of the Internal Affairs Ministry, Moscow, e-mail: m1va@yandex.ru

Konstantin M. Bondar – Cand. Sc. (Technical), Associate professor of the Information and Technical Department Far Eastern Law Institute of the Internal Affairs Ministry of Russia named after I.F. Shilov, Khabarovsk, e-mail: bondar_km@mail.ru