

и юридические действия. На их основе формируется рейтинг благонадежности, который определяет возможность получения доступа к сервисам и услугам. Вероятно, за некоторыми категориями граждан устанавливается более пристальное наблюдение. Крупные компании Китая, связанные со сферой информационно-телекоммуникационных технологий (такие как Alibaba, Baidu и др.), участвуют в этом эксперименте.

2. Аналитические и прогнозные модели. Во многих городах США внедрены системы, выявляющие тенденции на основе анализа данных и предсказывающие время и место совершения преступлений. При этом активно используются возможности частных компаний, которые совместно с полицейскими специалистами разрабатывают соответствующие системы (например, IBM создало систему Blue CRUSH (от англ. Crime Reduction Utilizing Statistical History – сокращение преступности с использованием статистических данных); Калифорнийский университет (UCLA) – систему PredPol, которая используется и в Великобритании; система криминального анализа в реальном времени – Real-time Intelligence Crime Analytics System (RICAS); решения Palantir Technologies собирают различную информацию (ДНК, записи систем видеонаблюдения и телефонных переговоров), отслеживают передвижения по номерным знакам арендованных машин и др.; система предупреждения преступлений Domain Awareness System собирает и анализирует информацию с камер видеонаблюдения и др.).

3. Осуществление цифровых расследований. Компанией Kimera Systems разработана система Nigel, накапливающая знания с учетом контекста. Она используется правоохранительными органами в цифровых расследованиях.

ForAllSecure и Университетом штата Пенсильвания создана система Mayhem, используемая ФБР для распознавания «почерка» хакеров.

4. Обеспечение коммуникации и взаимодействия. Еще одним направлением является привлечение социальных сетей, таких как Twitter и Facebook в США, Qzone, Penguou, WeChat в Китае. Правоохранительные органы все чаще полагаются на них для коммуникации с жителями.

Однако в последнее время часто возникают вопросы к используемым системам ИИ. Прогнозные системы обвиняют в том, что они концентрируют полицейские ресурсы в некоторых районах. Если же в одно место направлять больше полиции, как рекомендует ИИ, то там будет выявляться больше правонарушений, потому что такова работа полицейских, а не благодаря силе машинного обучения.

Кроме того, многих беспокоит отсутствие прозрачности при создании таких систем, надежность данных, используемых в них. Разработчики не разглашают данную информацию. Инструменты контроля не позволяют оценить имеющиеся риски.

Наконец, возникают проблемы, связанные с конституционными правами граждан, персональные данные которых собираются и обрабатываются ИИ.

Таким образом, на основе анализа зарубежного опыта использования ИИ можно сделать несколько предложений по использованию ИИ в раскрытии преступлений:

- интеграция имеющихся учетов для проведения интеллектуального анализа информации в целях раскрытия преступлений;
- развитие автоматизированных систем поиска и анализа контента в интернете;
- развитие комплексных систем, способных в режиме реального времени проводить идентификацию граждан по биометрическим данным или прогнозировать их поведение;
- развитие систем планирования и принятия управленческих решений, в том числе в оперативно-розыскной сфере;
- развитие аналитических систем профилактики, как общей, так и частной;
- использование систем ИИ, имеющихся в коммерческих и государственных структурах, для целей оперативно-розыскной деятельности (банки, социальные сети, мессенджеры, интернет-магазины и провайдеры и т. п.).

УДК 34

П.И. Иванов

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ НАУКИ НА СОВРЕМЕННОМ ЭТАПЕ

Рассматривая оперативно-розыскную науку как относительно самостоятельную отрасль знания, невольно вспоминаются слова А. Суворова: «теория без практики мертва, практика без теории слепа». Особенно последнее словосочетание «практика без теории слепа» уже дает о себе знать правоохранительной деятельности, для которой теория оперативно-розыскной деятельности (ОРД), а теперь целая наука была и остается своеобразной «подушкой безопасности». Разработанные ею предложения и рекомендации существенно снижали затраты (издержки), связанные с противодействием преступности. Уже сегодня, в несколько «обновленном» виде, звучат нами воспроизведенные слова А. Суворова: «нет ничего практичнее, чем хорошая теория». Подчеркивается особая значимость теории, в том числе ОРД, которую она заслужила, накопив в свой арсенал испробованные практикой средства и методы борьбы с криминальными проявлениями. Однако оперативно-розыскная наука и сегодня не исчерпала свой потенциал, в ней остро нуждается правоприменительная практика, поскольку можно даже на одном из признаков, ее характеризующих, убедиться в ее действенности. В данном случае мы имеем в виду самодостаточность оперативно-розыскных механизмов для своевременного реагирования на негативное изменение криминогенной ситуации. Многолетняя практика показывает, что любые коренные преобразования, крутые переломы в жизни общества всегда сопровождаются ростом преступности.

Как мы полагаем, в настоящее время остро нуждаются на предмет определения «реперных» точек, связанных с поиском эффективных средств и методов борьбы с преступлениями экономической и коррупционной направленности, в теоретическом осмыслении ведомственной наукой следующие вопросы:

современное представление о методологии рассматриваемой науки и ее структуры (предмет, объект, принципы, язык и т. д.);

использование криптовалюты при совершении преступлений экономической направленности;
механизм адаптации искусственного интеллекта (Больших данных) в интересах оперативных подразделений полиции;
противодействие киберпреступлениям;
приобретение организованной преступностью черт транснационального социально-правового явления;
активное участие в реализации государственной политики в области защиты прав и законных экономических интересов предпринимателей от преступных посягательств.

Перечень приведенных преобразований, произошедших в обществе и требующих теоретического осмысления, безусловно, не исчерпывающий. На наш взгляд, указаны лишь наиболее значимые из них, которые должны изучаться в первоочередном порядке специалистами рассматриваемой области науки.

Ощущается некоторое отставание от оперативно-розыскной практики самой ведомственной науки. Отчасти случилось такое положение из-за резкого «омоложения» специалистов, нарушения принципа преемственности.

Восполнить упущенное, по нашему мнению, возможно посредством объединения усилий ученых научных и образовательных организаций различных ведомств, структурные подразделения которых правомочны осуществлять в соответствии с Федеральным законом Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» оперативно-розыскную функцию.

Возвращаясь к внедрению современных информационных технологий в ОРД органов внутренних дел, полагаем необходимым создать по крайней мере следующие взаимосвязанные условия:

нормативно-правовое регулирование общественных отношений, возникающих в сфере использования в ОРД передовых информационно-телекоммуникационных технологий, информационных систем в целях сбора, обработки, внесения, хранения и использования оперативно значимой информации о предметах, событиях, представляющих оперативный интерес объектах, для предупреждения, раскрытия и расследования преступлений;

разработка и внедрение компьютерных программ, специально рассчитанных на переход к цифровой технологии оперативно-служебной деятельности оперативных подразделений полиции;

обеспечение защиты информации от несанкционированного доступа (копирования, уничтожения, распространения и любых других незаконных операций с хранящимися данными).

На основе выборочного изучения проблемы мы приходим к выводу, что внедрение современных информационных технологий в деятельность оперативных подразделений полиции (на сегодня их 12) способствует:

технической автоматизации отдельных процессов подготовки, принятия и реализации управленческих решений в рамках полномочий (компетенции) указанных подразделений;

созданию единой системы информационно-аналитического обеспечения их деятельности (централизованных баз данных, единой инфраструктуры, технологии регламентированного доступа к базам данных);

обеспечению информационного взаимодействия (электронного) между оперативными и иными подразделениями полиции, а также с другими правоохранительными органами и органами, осуществляющими ОРД;

повышению эффективности принимаемых управленческих решений по ключевым направлениям оперативно-служебной деятельности оперативных подразделений полиции (борьба с тяжкими и особо тяжкими преступлениями, их документирование, оперативное сопровождение расследования и т. п.);

использованию в установленном порядке (по мере необходимости) электронного документооборота, чтобы разгрузить большой объем документопотоков, так как объем несекретного документооборота, адаптированного к электронному документообороту, не уменьшается, хотя процесс оптимизации документооборота при подготовке, принятии и реализации управленческих решений продолжает оставаться не менее важной задачей;

внедрению унифицированных прикладных решений по основным направлениям оперативно-служебной деятельности оперативных подразделений полиции.

Вышеуказанный перечень преимуществ заставляет задуматься о необходимости ускоренного масштабного внедрения информационно-телекоммуникационных технологий в деятельность оперативных подразделений полиции. При этом мы придерживаемся мнения о предварительном создании теоретической модели реализации такого нововведения, учитывая специфический характер функций, осуществляемых указанными подразделениями. Разумеется, при решении данной задачи не обойтись без учета достижений оперативно-розыскной науки.

Таким образом, научное обеспечение оперативно-розыскной деятельности оперативных подразделений полиции как разновидности правоохранительной деятельности невозможно без дальнейшего развития ведомственной оперативно-розыскной науки.

УДК 342 + 004

А.В. Ивановский

ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОГО ПОТОКА ДЕСТРУКТИВНЫХ СООБЩЕНИЙ В ЭЛЕКТРОННЫХ СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ И СОЦИАЛЬНЫХ СЕТЯХ

Концепция информационной безопасности Республики Беларусь, отечественные и зарубежные исследования отмечают факт массивного, возрастающего по интенсивности и токсичности деструктивного информационного воздействия на белорусское общество. С учетом этого правовая оценка характеристик и фиксация юридически значимых маркеров в