Как отмечает А.Г. Лекарь, пресечение преступлений – выявление лиц, подготавливающих совершение преступления, и принятие к ним мер (главным образом оперативно-розыскных) в целях недопущения перерастания приготовительных действий в покушение, а покушения – в оконченное преступление. В предложенной ученым дефиниции прослеживается четкая взаимосвязь с профессиональной деятельностью непосредственно оперативных подразделений.

Надо полагать, что, придерживаясь вышеуказанной позиции, Н.И. Журавленко, А.Н. Халиков, Е.Н. Яковец уточняют данное понятие словосочетанием «это действия органов, осуществляющих ОРД», тем самым подчеркивая терминологическую специфику.

Несколько другой интерпретации придерживается В.В. Голина, определяя пресечение преступлений как совокупность видов деятельности, направленной на прекращение начатого преступления путем разработки и осуществления специальных мероприятий.

Несмотря на определенные противоречия, имеющиеся во взглядах ученых, большинство из них едины во мнении, что пресечение осуществляется исключительно на стадиях приготовления и покушения. Данная точка зрения полностью разделяется и нами.

Вместе с тем не вызывает сомнений, что на практике существуют трудности с документированием приготовлений к совершению хищений на предприятиях легкой промышленности, связанных с посягательством на сырье и готовую продукцию, поэтому оперативные сотрудники стремятся занять позицию выжидания, например в целях задержания фигурантов с поличным в момент вывоза товарно-материальных ценностей. Это обусловлено необходимостью подтверждения противоправного умысла и минимизации риска уклонения фигурантов от уголовной ответственности.

Кроме того, фактор внезапности задержания с поличным приводит лиц, участвующих в преступной деятельности, к растерянности, создавая благоприятные условия для установления с ними оперативного контакта и получения дополнительных сведений о ранее неизвестных эпизодах совершенных общественно опасных деяний, а также о неустановленных фигурантах, оказывающих содействие в совершенных преступлениях, и т. п.

Следует отметить, что вышеуказанный подход не лишен недостатков и разделяется не всеми учеными. В частности, В.Д. Иванова полагает, что отдельные сотрудники органов внутренних дел вместо совершенствования своего профессионального мастерства, использования достижений науки и техники становятся на ошибочный путь, т. е. стремятся

заполучить как можно больше доказательств о преступной деятельности виновных, дают возможность приготовлению перерасти в непосредственное посягательство и только после этого пресекают содеянное на стадии покушения.

На наш взгляд, промедление в принятии решительных мер может привести к созданию негативных последствий: причинению материального ущерба в особо крупном размере, уничтожению либо сокрытию документов и других материальных носителей со следами хищений на предприятии легкой промышленности, исчезновению самих фигурантов, например выезд за границу. Все перечисленное существенно затрудняет или вовсе исключает целесообразность проведения некоторых оперативно-розыскных мероприятий. Как итог, лицам, совершающим рассматриваемую группу преступлений, удается избежать уголовной ответственности.

Для недопущения подобных негативных тенденций в современных условиях оперативному сотруднику необходимы умения действовать в различных для него оперативно-розыскных ситуациях, которые по сущности определяют решаемую задачу, а именно предупреждение, пресечение или выявление хищений на предприятиях легкой промышленности.

В этой связи следует разрабатывать научно обоснованные рекомендации по принятию наиболее эффективных организационно-тактических решений и в части пресечения вышеуказанных общественно опасных деяний, акцентируя внимание на изучении соответствующей оперативно-розыскной характеристики общественно опасных деяний, раскрывающей в полной мере способ совершения преступления от его подготовки, совершения и до сокрытия, а также поведенческие особенности личности преступника на каждом из отмеченных этапов данного способа, в том числе учитывая особенности предмета преступного посягательства.

УДК 343.985.8:004

А.В. Черецких

АВТОМАТИЗИРОВАННЫЕ УЧЕТЫ И БАЗЫ ДАННЫХ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

На современном этапе развития общества информатизация внедрена во все сферы, в том числе в деятельность правоохранительных органов при раскрытии, расследовании и предупреждении преступлений. Таким образом, указанная деятельность в условиях развития информационно-

коммуникационных технологий невозможна без их внедрения фактически во все ее процессы.

В настоящий момент при раскрытии, расследовании и предупреждении преступлений применяются как универсальные, так и специальные программы и программные комплексы.

В оперативно-розыскной деятельности широко применяются централизованные и региональные оперативно-справочные, розыскные и криминалистические учеты (всего насчитывается свыше 50 видов учетов), многие из которых используются повсеместно, другие – единично на местном или региональном уровне. Наиболее распространены дактилоскопические автоматизированные учеты, или автоматизированные дактилоскопические информационные системы (АДИС) («Сонда-Фрес» и «Папилон»); автоматизированные системы учета лиц по элементам внешности (АИРС) («ИКР-2», «Портрет», «ФОТОРОБОТ», «КРИС»); автоматизированные информационно-поисковые системы, из которых состоят учеты (АИПС) «Картотека» (автоматизированный пофамильный и дактилоскопический учет служит для получения сведений о гражданах Российской Федерации, иностранцах и лицах без гражданства; судимости, месте и времени отбывания наказания, дате и основании освобождения, смерти в местах лишения свободы, изменении приговора, амнистии; месте жительства и месте работы до осуждения; розыске лиц, задержанных за бродяжничество; перемещении осужденных; группе крови, дактилоскопической формуле), «Оружие» (позволяет вести учет утраченного (похищенного, утерянного) и выявленного (изъятого, найденного, добровольно сданного) вооружения (стрелковое оружие, гранатометы, артиллерийские системы и др.)), «Автопоиск», «Вещь» (информирует пользователя о похищенных и изъятых номерных вещах, а также документах, ценных бумагах общего государственного обращения в связи с совершенными преступлениями), «Антиквариат» и т. д.

В системе МВД России сконцентрирован большой объем информации, используемой в служебных целях, что приводит к формированию и ведению всевозможных банков данных и созданию систем управления базами данных, которые отвечали бы требованиям МВД России при выполнении служебных задач. Перечисленные выше учеты являются составной частью банков данных. Сама структура системы информационного обеспечения чаще подразделяется на четыре уровня: территориальный, региональный, межрегиональный и федеральный. Ниже перечислены эксплуатируемые в настоящее время системы и банки: автоматизированная информационная система «Криминал-И» (для учета правонарушений, совершенных иностранцами и лицами без гражданства); программный комплекс «Легенда-Мерилиан»; автоматизированная подсистема «Административная практика»; «Розыск-Магистраль»; интегрированный банк данных регионального уровня (ИБД-Р); интегрированный банк данных федерального уровня (ИБД-Ф).

Информатизация процессов обработки и хранения оперативно значимой информации ускоряет ее поиск, что, в свою очередь, позволяет оперативно принять действенные меры при раскрытии, расследовании и предупреждении преступлений. Однако имеется один существенный недостаток информатизации процессов оперативно-розыскной деятельности, заключающийся в отсутствии интеграции всех учетов, баз и банков данных.

В нормативных правовых актах, регламентирующих информатизацию и применение информационных технологиях, все зафиксировано грамотно и достаточно подробно. Однако на деле выходит, что при проведении оперативно-розыскных мероприятий сотруднику необходимо просмотреть все возможные учеты и банки данных, к которым у него есть доступ, чтобы получить интересующую информацию о субъекте, а если она отсутствует, то внести эту информацию. Не исключен также человеческий фактор, который заключается в опечатках и невнимательности сотрудников при обработке сведений в информационных системах. Кроме того, обращение к тому или иному виду учета может быть ограничено из-за территориальных уровней подсистем, и сотрудник может получить ложно отрицательный результат в ходе запроса. Таким образом, процесс сбора данных из информационных систем, который должен был бы занимать не более 5 мин, может занимать в десятки раз больше времени и нередко быть нерезультативным.

Запущенная в 2013 г. единая система информационно-аналитического обеспечения деятельности МВД России, другими словами интегрированная система обработки данных (ИСОД), частично решает эти задачи, но пропускная способность каналов связи, а на некоторых удаленных территориях и вовсе отсутствие зон покрытия и поставщиков услуг связи затрудняют работу с ней. Основная цель ИСОД – повышение уровня информационно-аналитического обеспечения МВД России. Указанная цель достигается решением следующей задачи: совершенствование правовых, нормативно-технических, организационно-методических и иных основ разработки, внедрения, эксплуатации и развития ИСОД МВД России и ее компонентов.

Что касается анализа и обработки информации в подсистемах и сервисах ИСОД МВД России, то данная задача пока не решена.

Для исключения подобных проблем требуется глобальная интеграция и изменение самой структуры информационного обеспечения. Гло-

бальная интеграция всех учетов и банков позволит незамедлительно проводить автоматизированный анализ обнаруженных объектов и следов с объектами и следами, имеющимися в информационной системе. В результате будет исключена необходимость перехода из одного банка данных в другой или из одного учета в другой с прохождением каждый раз процедуры авторизации. При реализации глобальной интеграции всех учетов и банков данных получаемая информация действительно станет оперативной и значимой. Реализация логической взаимосвязи компонентов глобальной интегрированной системы позволит повысить информированность каждого сотрудника, предоставит условия для более эффективного использования накопленной информации в процессе расследования, раскрытия и профилактики преступлений. Анализ связей компонентов (следов, объектов и субъектов) системы будет проще, а применение математических алгоритмов (на основе искусственного интеллекта) позволит этот процесс автоматизировать, что во много раз сократит аналитическую работу сотрудников по построению связей.

Информационная безопасность при формировании глобального интегрированного банка данных может обеспечиваться многоуровневой системой защиты, быть подобной имеющимся средствам защиты. Обеспечение информационной безопасности при работе с персональными данными субъектов также может быть организовано имеющими способами, но дополнено обезличиванием, а именно: пока объекты не будут идентифицированы, вся информация о них будет закодирована. Как только произошла идентификация объектов по заранее определенным признакам, кодировка снимается, в дополнение на служебную почту сотрудника поступает единоразовый код доступа и сотрудник получает полный доступ к информации. Данный способ позволит исключить использование служебной информации в личных целях и будет являться дополнительным уровнем защиты.

УДК 343.985

А.И. Чурносов, В.В. Тропин

НЕКОТОРЫЕ ОСОБЕННОСТИ ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Исследование компьютерной информации является одним из самых молодых направлений в криминалистической технике, которое начало складываться в первой половине 90-х гг. XX в. В настоящее время указанные исследования проводятся почти по всем категориям уголовных

дел. Наиболее часто компьютерная информация исследуется при расследовании преступлений в сфере компьютерной информации; терроризма и экстремизма, экономических и налоговых преступлений; распространения порнографической продукции; преступных нарушений авторских и смежных прав; изготовления поддельной печатной продукции (например, бланков документов, денежных знаков, ценных бумаг). В последние годы значительно выросло число исследований компьютерной информации в ходе раскрытия преступлений против личности. Экспертизы компьютерной информации стали повседневным явлением при рассмотрении как гражданских дел, так и дел об административных правонарушениях.

Компьютерная информация является объектом материального мира, элементом искусственной среды, созданным человеком. Она может существовать только с помощью специальных технических средств – электронно-вычислительной техники и электронных средств связи (систем телекоммуникаций).

Компьютерная информация, как и любой другой вид информации, состоит из двух элементов: содержания (сведения о каком-либо явлении объективной реальности) и материального носителя данных сведений.

Содержание компьютерной информации представлено в форме, пригодной для обработки ЭВМ, ее материальным носителем является электромагнитное поле. В свою очередь, носитель электромагнитного поля может быть материально-фиксированным предметом (жесткий диск, съемные магнитные носители) и не иметь предметной формы (передача информации по беспроводным каналам в компьютерных сетях, например Wi-Fi).

Природа компьютерной информации обусловливает следующие ее свойства, делающие ее весьма сложным объектом криминалистического исследования: компьютерная информация недоступна для непосредственного человеческого восприятия; определенное содержание информации не может быть однозначно закреплено за конкретным материальным носителем; материальный носитель компьютерной информации (электромагнитное поле) невозможно индивидуализировать; содержание информации может быть отделено от ее материального носителя без взаимных изменений; изменение содержания компьютерной информации не вызывает изменений ее носителя, и наоборот; можно быстро обрабатывать, изменять и удалять информацию, в том числе путем удаленного доступа, вне контроля лиц, правомерно пользующихся данной информацией; не всегда возможно восстановить первоначальное содержание измененной или удаленной информации.