СИСТЕМА "РОЗЫСК-МАГИСТРАЛЬ" В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА ТРАНСПОРТЕ

К.т.н, доцент, А.В. Бочкарев, к.т.н., В.В. Сластенов (Саратовский юридический институт МВД России), Е.В. Морозова (Приволжское УВД на транспорте МВД России)

В соответствии с Федеральным законом "Об оперативно-розыскной деятельности" от 12 августа 1995г. основными задачами, стоящими перед субъектами ОРД, являются выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших, осуществление розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания и розыска без вести пропавших.

В современных условиях эффективное выполнение этих задач невозможно без использования автоматизированных информационно-поисковых систем (АИПС) оперативно-розыскного назначения.

Основной АИПС, действующей в ОВД на транспорте, является программно-технический комплекс (ПТК) "Розыск-Магистраль". Этот комплекс начал внедряться в оперативно-служебную деятельность в 2000 году в соответствии с приказами МВД России №980-1999 г., №1070-1999 г. и "Целевой программой внедрения программно-технического комплекса "Розыск-Магистраль" в ОВД на транспорте МВД России".

ПТК "Розыск-Магистраль" предназначен для выполнения в автоматизированном режиме следующих функций:

- выявления в пассажиропотоке лиц, находящихся в розыске, а так же лиц, представляющих оперативный интерес для правоохранительных органов, посредством автоматического сравнения баз данных по лицам, находящимся в федеральном и местном розыске, лиц представляющих оперативный интерес, утраченных и похищенных документов и д.р. с транспортными базам данных;
- круглосуточного пополнения баз данных информацией, поступающей из ОАО "РЖД", его филиалов и структурных подразделений; предприятий авиатранспорта; ГИАЦ МВД России; информационных центров МВД, ГУВД, УВД, УВДТ; подчиненных линейных подразделений и других правоохранительных органов;
- предоставления возможности поиска по базам данных АИПС в различных режимах;
- выгрузки данных из информационных массивов АИПС и их передачи их в вышестоящие подразделения для формирования общероссийского (межрегионального) информационного массива;
- осуществления по запросу пользователя аналитической обработки имеющейся в базах данных ПТК информации с целью выявления и раскрытия преступлений в сфере пассажирских перевозок;
- проведения аналитических разработок по регистрируемым преступлениям и делам оперативного учета;
- формирования статистической отчетности о результатах работы системы как по выявлению лиц, находящихся в розыске и предоставляющих оперативный интерес, так и по количеству и качеству выданной информации по запросам пользователей.

Помимо описанных выше функций, в системе "Розыск-Магистраль" реализовано использование программных модулей – автоматизированных рабочих мест (АРМ), позволяющих выявлять и раскрывать преступления, совершенные в сфере пассажирских перевозок. В основу работы аналитических модулей заложен принцип отраслевой интеграции информации. Для каждого направления работы (по линии уголовного розыска, борьбы с незаконным оборотом наркотиков, борьбы с организованной преступностью и др.) существует свой АРМ, позволяющий посредством специально разработанных алгоритмов извлекать из общего банка информации и анализировать данные, необходимые для выявления и раскрытия конкретных видов преступлений.

Алгоритм обработки информации в ПТК "Розыск-Магистраль" представлен на рис.1.

Для информационной поддержки нарядов патрульно-постовой службы и оперативных сотрудников служат мобильные терминалы ПТК "Розыск-Магистраль". Эти терминалы представляют собой карманные персональные компьютеры и предназначены для оперативного доступа сотрудников правоохранительных органов к информации баз данных федерального и регионального уровней, таких как: "Розыск лиц", "Паспорта", "Оружие", "Угон" и др.

Мобильные терминалы позволяют:

- выявлять лиц, находящихся в федеральном или местном розыске, представляющих интерес, использующих документы, числящиеся как утраченные или похищенные;
- выявлять автотранспорт, находящийся в розыске;
- осуществлять контроль над перевозками подакцизных товаров железнодорожным транспортом.

Мобильные терминалы системы "Розыск-Магистраль" работают с ежедневно обновляющейся локальной базой данных или могут осуществлять доступ к серверу баз данных в режиме реального времени по существующему каналу связи, в том числе и с применением WEB - технологий.

Рассмотрим использование ПТК "Розыск-Магистраль" на примере Приволжского УВДТ. Информация о лицах, приобретавших проездные документы на поезда дальнего следования Поволжского региона, 7 раз в

сутки получаются с сервера "ЭКСПРЕСС" Информационно-вычислительного центра Приволжской железной дороги. За сутки по системе "Розыск-Магистраль" проверяется порядка 45-55 тыс. человек. Ежегодно с использованием АИПС на территории обслуживания Приволжского УВДТ задерживается порядка 300 человек, находящихся в розыске.

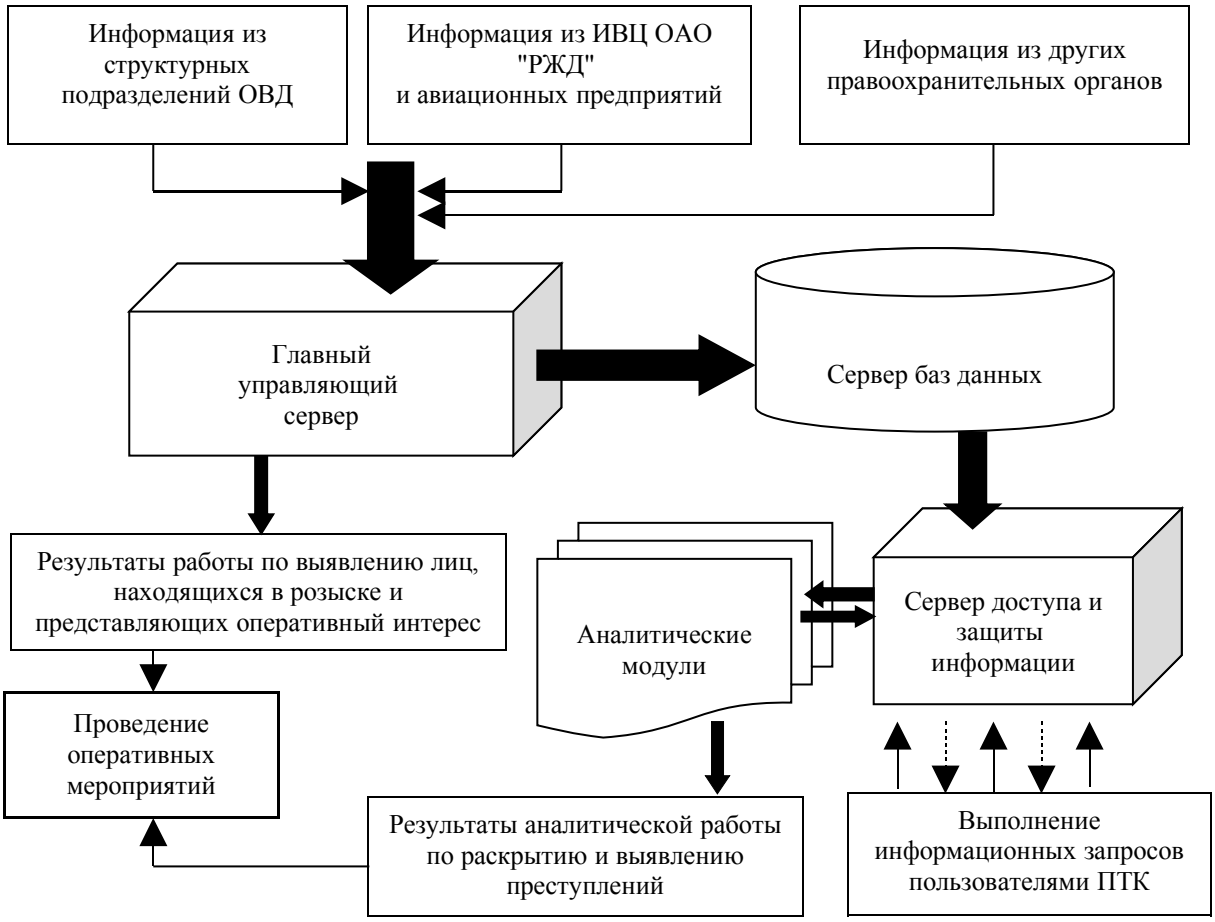

Рис. 1. Алгоритм обработки информации в ПТК "Розыск-Магистраль"

Большую пользу в выявлении и задержании лиц, скрывающихся от следствия и суда обеспечивает система сторожевого контроля за перемещением лиц, представляющих оперативный интерес. Приведем конкретный пример из практической деятельности ОВДТ.

В августе 2005 г. группа боевиков в составе 8 человек, среди которых находились братья Башаевы, входящие в незаконное вооруженное формирование, осуществила вооруженное нападение на домовладение главы администрации с. Рошни-Чу Урус-Мартановского района Чеченской республики Бексултанова Б.Ш. В результате нападения был похищен его сын, а также убиты военный комендант Урус-Мартановского района, его заместитель и трое военнослужащих. Прокурором Чеченской республики было возбуждено уголовное дело по признакам преступлений, предусмотренных ч.3 ст. 30, ст. 105 ч.2 п. "а, б, е, ж, з", ст. 126 ч.3 п. "а", ст. 205 ч.3, ст.209 ч.2, ст. 222 ч.3, ст. 317, ст. 167 ч.2 УК РФ.

Сотрудниками ЦОРИ Приволжского УВДТ сведения о братьях Башаевых были занесены в базу данных сторожевого контроля ПТК "Розыск-Магистраль".

В начале марта 2006 года было выявлено, что гражданин Башаев В.Ш. приобрел железнодорожный билет на поезд №67 и собирается выехать со станции Волгоград-1 до станции Брест-Центральный.

04.03.2006 г. в 08:45 в ходе проведения оперативно-розыскных мероприятий сотрудниками Волгоградского ЛУВДТ в зале ожидания железнодорожного вокзала станции Волгоград-1 лидер бандформирования гражданин Башаев Висхан Шамханович, 1988 года рождения, кличка "Абдулла", проживающий по адресу Чеченская республика, с. Катар-Юрт ул. Ленина д. 15 и пытавшийся выехать в республику Беларусь, был задержан. Для проведения следственных действий и оперативно-розыскных мероприятий Башаев В.Ш. был передан сотрудникам оперативно-розыскного бюро Главного управления по Южному федеральному округу МВД России.

В настоящее время автоматизированная информационно-поисковая система ПТК "Розыск-Магистраль" функционирует практически во всех УВДТ МВД России. В 2006 году с использованием данного комплекса проверено свыше 699 млн. человек, приобретавших проездные документы на железнодорожный и авиационный

транспорт. В результате проведенных мероприятий было задержано около 17 тыс. человек, находившихся в розыске и обоснованно подозреваемых в совершении преступлений.

Наиболее эффективно система используется в Северо-Кавказском и Среднеуральском УВДТ. Так, в 2006 году с помощью информационной системы "Розыск-магистраль" на Северо-Кавказской магистрали проверено более 215 миллионов человек, в результате выявлено 1140 человек, находящихся в федеральном розыске, и более 1220 человек - в местном.

Органы внутренних дел на транспорте оказывают содействие и правоохранительным органам стран СНГ в установлении и задержании разыскиваемых лиц. С использованием ПТК "Розыск-Магистраль" в 2006 году задержано 523 лица, находящихся в межгосударственном розыске.

Приведенные примеры, по нашему мнению, убедительно показывают, насколько важным аспектом работы оперативных подразделений в настоящее время является использование компьютерных технологий в оперативно-розыскной деятельности.

Вместе с тем следует признать, что далеко не все возможности ПТК "Розыск-Магистраль" используются достаточно эффективно и в полном объеме.

На эффективность работы системы "Розыск-Магистраль" отрицательно сказывается разнообразие документов, по которым могут приобретаться проездные документы на железнодорожный и воздушный транспорт и смена паспортов при достижении гражданином определенного возраста. На наш взгляд эффективность поиска лиц, находящихся в розыске и представляющих оперативный интерес, в пассажиропотоке была бы значительно выше, если бы на территории России действовала система персональной идентификации гражданина. Данная система построена не на фамилии, имени и отчестве человека, а на уникальном числовом коде, который присваивается ему один раз и обеспечивает однозначную идентификацию гражданина независимо от предъявляемого им документа, например, так как это осуществляется в ряде государств СНГ. Другим возможным вариантом является использование для идентификации личности биометрических данных, но при этом возникает проблема перевода биометрических данных в числовую форму, пригодную для автоматизированного поиска.

ИСПОЛЬЗОВАНИЕ МНОГОМЕРНЫХ БАЗ ДАННЫХ ПРИ ПОСТРОЕНИИ ИНФОРМАЦИОННЫХ СИСТЕМ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ КРИМИНАЛЬНОЙ МИЛИЦИИ

Волгин Ю. Г., старший преподаватель (Кемеровский филиал Омской академии МВД России)

Задачей информационного обеспечения подразделений криминальной милиции является удовлетворение возникающих у них информационных потребностей. При рассмотрении подобного рода потребностей нам представляется целесообразным обратиться к характеристике информационных процессов, протекающих при осуществлении оперативно-розыскной деятельности. Такие процессы можно представить как последовательность следующих взаимосвязанных этапов: получение, обработка, представление, хранение, передача оперативно-розыскной информации, а также ее реализация[1].

Из всех перечисленных на наш взгляд следует более подробно остановиться на этапе обработки оперативно-розыскной информации. Характеризуя отмеченный этап, следует указать на то, что имеющиеся в распоряжении оперативных подразделений криминальной милиции данные и сведения требуют систематического анализа. А при решении многих из задач, возникающих в процессе оперативно-розыскной деятельности, есть необходимость аналитической обработки значительных объемов информации. На наш взгляд следует согласиться с утверждением о том, что "человеческий разум сам по себе не приспособлен для восприятия больших массивов информации. Человек к тому же не способен улавливать более двух-трех взаимосвязей даже в небольших выборках"[2]. Подобный анализ оперативно-розыскной информации должен осуществляться сотрудниками оперативных подразделений криминальной милиции с использованием информационных систем. На необходимость такого анализа, как возможной функции информационной системы, указали 84,8 % опрошенных сотрудников оперативных подразделений криминальной милиции.

Подчеркивая необходимость автоматизации аналитической обработки информации, получаемой и систематизируемой в процессе осуществления оперативно-розыскной деятельности, по нашему мнению, следует согласиться с мнением В. А. Филиппова, утверждающего, что "объемы данных, требующие оперативного анализа, привели к необходимости создания аналитических систем, позволяющих отвечать на вопросы, в которых эти данные рассматриваются с различных сторон"[3].

Отмеченные обстоятельства обуславливают целесообразность рассмотрения вопросов построения информационных систем, предназначенных для оперативных подразделений криминальной милиции, и, в частности, для решения задач аналитической обработки оперативно-розыскной информации.

---

[1] Подробнее см.: *Волгин Ю. Г.* Оперативно-розыскная деятельность как информационно-познавательный процесс / Ю. Г. Волгин // Милиция Сибири: история и современность: материалы региональной научно-практической конференции, посвященной 200-летию МВД. Кемерово, 26 марта 2002 г. – Кемерово, 2002. – С. 153-159.

[2] *Филиппов В. А.* Интеллектуальный анализ данных: методы и средства / В. А. Филиппов. – М., 2001. – С. 6.

[3] *Филиппов В.А.* Язык XML и многомерная СУБД D^3 / В. А. Филиппов, Б. А. Щукин, А. В. Постоянов. – М., 2001. – С. 30.

Характер поисковых и аналитических задач решаемых на трех уровнях в процессе осуществления оперативно-розыскной деятельности раскрывает С. С. Овчинский. К числу таких задач он относит:

- на управленческом уровне: изучение оперативной обстановки; обобщение данных об условиях, способствующих совершению преступлений и разработка мер общей профилактики;
- на организационно-тактическом уровне: выбор эффективных методов индивидуальной профилактики и анализ ее результатов; обобщение данных о двух или нескольких преступлениях, предположительно совершенных одними и теми же лицами; анализ информации о силах и средствах оперативно-розыскной деятельности;
- на оперативно-тактическом: обнаружение преступников по приметам, элементам способа совершения преступлений, путем отождествления личности; установление причастности к ранее совершенным и оставшимся нераскрытыми преступлениям лиц, проверяемых оперативно-розыскными средствами и методами; получение справок и необходимой информации о лицах, состоящих на оперативно-розыскном учете. [4]

Решение указанных задач предполагает использование определенных методов анализа и получение на основе этого новых знаний. Однако, глубоко укоренившийся в настоящее время подход к решению задач анализа путем использования методов традиционной математики[5] в ходе аналитической обработки оперативно-розыскной информации эффекта не дает, поскольку вступает в действие принцип несовместимости Л. Заде, согласно которому "с ростом сложности систем человеческая способность делать точные утверждения о них падает"[6]. Характеризуя возможности статистического анализа, нам представляется необходимым, отметить, что традиционная математическая статистика, не имея необходимого математического аппарата, также неприменима для аналитической обработки оперативно значимой информации. Совершенно прав, по нашему мнению, В. А. Филиппов, утверждающий, что математическая статистика "оперирует усредненными характеристиками, которые часто являются фиктивными величинами"[7].

Более эффективным при аналитической обработке данных, в процессе осуществления оперативно-розыскной деятельности, может оказаться применение методов интеллектуального анализа данных. Данной группе методов, возможность использования которой до недавнего времени рассматривали лишь специалисты в технической[8] и экономической[9] областях, сейчас привлекают внимание и специалистов науки оперативно-розыскной деятельности, занимающихся вопросами аналитической разведки. В обоснование возможности и необходимости использования этой группы методов следует привести мнение Дж. Клира, который утверждает, что в отличие от традиционной математики, решающей задачи организованной простоты и математической статистики, решающей задачи неорганизованной сложности, с помощью методов интеллектуального анализа данных можно решать задачи так называемой организованной сложности[10]. Именно к задачам подобного рода и относится задача анализа оперативно-розыскной информации в процессе осуществления оперативно-розыскной деятельности.

Отмечая необходимость использования методов интеллектуального анализа данных, некоторые авторы указывают на такие их возможности как проверка гипотез и поиск неявных зависимостей[11].

В. А. Филиппов выделяет следующие пять основных типов закономерностей предметной области, которые можно выявить методами интеллектуального анализа данных:

- ассоциация;
- последовательность;
- классификация;
- кластеризация;
- прогнозирование[12].

В. В. Корнеев, А. Ф. Гареев, С. В. Васютин, В. В. Райх указывают целый ряд задач, которые можно решить с помощью методов интеллектуального анализа данных[13]. Среди них наиболее интересными в

---

[4] См.: *Овчинский С. С.* Оперативно-розыскная информация / С. С. Овчинский. – М., 2000. – С. 101-102.

[5] См., например: *Зубов И. Н.* Организация информационно-аналитической работы в органах внутренних дел: Методическое пособие / И. Н. Зубов, В. Ю. Попков, А. П. Титов, В. Н. Тищенко. – М., 1998.

[6] Цит. по кн.: *Ярушкина Н. Г.* Основы теории нечетких и гибридных систем: Учебное пособие / Н. Г. Ярушкина. – М., 2004. – С.16.

[7] *Филиппов В. А.* Интеллектуальный анализ данных: методы и средства / В. А. Филиппов. – М., 2001. – С. 6.

[8] См., например: *Усков А. А.* Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика / А. А. Усков, А. В. Кузьмин. – М., 2004. – С. 90-123; *Горелик А. Л.* Методы распознавания: Учебное пособие для вузов / А. Л. Горелик, В. А. Скрипкин. – М., 2004. – С. 161-190.

[9] См., например: *Филиппов В. А.* Многомерные СУБД при создании корпоративных информационных систем / В. А. Филиппов. – М., 2001. – С. 49-55.

[10] См.: *Ярушкина Н. Г.* Основы теории нечетких и гибридных систем: Учебное пособие / Н. Г. Ярушкина. – М., 2004. – С.16.

[11] См.: *Корнеев В. В.* Базы данных. Интеллектуальная обработка информации / В. В. Корнеев, А. Ф. Гареев, С. В. Васютин, В. В. Райх. – М., 2001. – С. 103.

[12] См.: *Филиппов В. А.* Интеллектуальный анализ данных: методы и средства / В. А. Филиппов. – М., 2001. – С. 8-9.

аналитической деятельности в процессе осуществления оперативно-розыскной деятельности, по нашему мнению являются:

- выделение в данных групп, сходным по некоторым признакам, т.е. задача кластерного анализа;
- нахождение и аппроксимация зависимостей, связывающих анализируемые параметры или события;
- поиск данных, существенно отклоняющихся от выявленных закономерностей (анализ аномалий);
- прогнозирование развития объектов различной природы на основе хранящейся ретроспективной информации об их состоянии в прошлом.

В. А. Филиппов приводит следующую классификацию методов интеллектуального анализа данных:

- предметно-ориентированная методология;
- статистические методы;
- нейронные сети;
- системы рассуждений на основе аналогичных случаев;
- деревья решений;
- эволюционное программирование;
- генетические алгоритмы;
- алгоритмы ограниченного перебора[14].

Следует указать, что, по нашему мнению, автор не вполне заслуженно обошел вниманием в таком перечислении методы нечеткой логики. А ведь именно они наряду с нейронными сетями и генетическими алгоритмами составляют основу того аппарата анализа, который Л. Заде назвал "мягкими вычислениями"[15] и который лежит в основе построения реально действующих интеллектуальных систем.

Сложность и разнообразие методов интеллектуального анализа данных требуют использования специализированных средств для решения задач аналитической обработки информации в процессе осуществления оперативно-розыскной деятельности. Общие требования к таким системам достаточно хорошо изложены в научной литературе[16]. Однако, оценка на соответствие данным требованиям, существующих и использующихся в настоящее время оперативными подразделениями криминальной милиции информационных систем, выявляет нецелесообразность их использования как средств автоматизации аналитической обработки оперативно-розыскной информации.

Так, большинство существующих автоматизированных информационных систем, используемых оперативными подразделениями криминальной милиции, относятся к классу информационно-поисковых систем, основным предназначением которых является накопление, хранение, а также обеспечение отбора и вывода информации по заданному в запросе условию. Данные системы позволяют частично автоматизировать также и этап обработки информации. Однако автоматизированной является только статистическая обработка, содержащихся в автоматизированной информационно-поисковой системе, данных, что подтверждается изучением практики их использования сотрудниками оперативных подразделений криминальной милиции.

Наряду с автоматизированными информационно-поисковыми системами оперативными подразделениями криминальной милиции также используются автоматизированные рабочие места. Автоматизированное рабочее место, по мнению М. П. Дубинина, должно своевременно удовлетворять информационные и вычислительные потребности специалиста[17]. Анализ практики использования автоматизированных рабочих мест позволяет установить, что удовлетворяются лишь потребности информационно-справочного характера и потребности представления информации в виде формализованных документов, что важно, однако не позволяет решить проблемы автоматизации аналитической обработки информации в процессе осуществления оперативно-розыскной деятельности.

Наряду с уже имеющимися информационными системами, некоторые специалисты, предлагают использование экспертных систем[18]. Подобные системы, отличительной особенностью которых является способность накапливать знания и опыт наиболее квалифицированных специалистов, должны:

- содержать алгоритмы оперативно-розыскных мероприятий по раскрытию отдельных видов преступлений;
- оптимизировать повседневные операции по подготовке служебных документов;

---

[13] См.: *Корнеев В. В.* Базы данных. Интеллектуальная обработка информации / В. В. Корнеев, А. Ф. Гареев, С. В. Васютин, В. В. Райх. – М., 2001. – С. 103.

[14] См.: *Филиппов В. А.* Интеллектуальный анализ данных: методы и средства / В. А. Филиппов. – М., 2001. – С. 9-18.

[15] См.: *Ярушкина Н. Г.* Основы теории нечетких и гибридных систем: Учебное пособие / Н. Г. Ярушкина. – М., 2004. – С. 9.

[16] См., например: *Барсегян А. А.* Методы и модели анализа данных: OLAP и Data Mining / А. А. Барсегян, М. С. Куприянов, В. В. Степаненко, И. И. Холод. – СПб., 2004. – С. 22.

[17] См.: *Информатика* и вычислительная техника в деятельности органов внутренних дел: Учебное пособие – М., 1996. – Ч. 4: Автоматизация решения практических задач в органах внутренних дел. – С. 10.

[18] См., например: *Горев А. И.* Создание экспертно-справочных систем как перспективное направление развития информационных технологий в деятельности ОВД / А. И. Горев // Подходы к решению проблем законотворчества и правоприменения: Межвузовский сборник трудов слушателей, адъюнктов, соискателей, аспирантов. – Омск, 1995. – С. 33-39.

- систематизировать хранение служебных документов и быстро получать различную справочную и нормативную информацию[19].

Очевидным является то, что данные системы можно использовать для удовлетворения потребностей в информации справочного и методического характера в процессе осуществления оперативно-розыскной деятельности, но вместе с тем нецелесообразно применять для автоматизации аналитической обработки оперативно-розыскной информации.

В научной литературе, наряду с рассмотренными видами информационных систем, раскрываются вопросы построения и применения систем оперативной аналитической обработки (OLAP – систем)[20]. Основным назначением данного класса систем является поддержка аналитической деятельности. И именно они, на наш взгляд, предоставляют реальную возможность автоматизации аналитической обработки оперативно-розыскной информации.

При разработке подобного рода информационных систем для оперативных подразделений криминальной милиции необходимо решить вопрос построения их баз данных. Обозначая в качестве ключевой проблему построения информационных массивов, мы полностью соглашаемся с позицией А. А. Барсегяна, М. С. Куприянова, В. В., Степаненко и И. И. Холода, утверждающих, что базы данных являются основой создания систем аналитической обработки данных[21].

Важным моментом, характеризующим информационные массивы, является модель представления данных, т.е. совокупность логических конструкций, используемых для представления структуры данных и отношений между ними внутри[22]. Нам представляется целесообразным сформулировать предложения по выбору модели представления данных. Для этого необходимо взять за основу некоторые из основных требований к информационным системам аналитической обработки информации. К таковым относятся:

- детализация хранимых данных. В системах анализа в большинстве случаев требуется выполнять обработку значительного количества данных с широким применением группировок и обобщений. Требуется хранение как детализированных, так и обобщенных данных;
- качество данных. Не допускаются ошибки в данных, которые при анализе могут привести к неправильным выводам;
- формат хранения данных. Требованием, предъявляемым к информационной базе систем анализа, является единый согласованный формат хранения данных, поскольку в процессе анализа различие форматов чрезвычайно затрудняет аналитическую обработку;
- допущение избыточности данных. Целью избыточности является упрощение схемы базы данных;
- характер запросов к данным. Для системы анализа невозможно заранее определить характер запросов, поэтому к ним предъявляется требование обеспечения произвольных запросов к базам данных лиц, осуществляющих аналитическую обработку[23].

Помимо отмеченных, нам представляется целесообразным указать также требование, сформулированное П. Робом и К. Коронелом, а именно точное соответствия реальному миру[24].

В настоящее время при построении баз данных в информационных системах, применяемых оперативными подразделениями криминальной милиции, используются различные модели представления данных. Необходимо оценить такие модели на соответствие предъявляемым требованиям.

Так, при построении баз данных информационных систем, как правило, используется реляционная модель. Данная модель наиболее часто используется и при формировании массивов оперативно значимой информации в органах внутренних дел, что обусловлено рядом причин. Подробно такие причины с технических позиций рассматривает А. И. Змитрович[25]. И среди них, на наш взгляд следует указать на простую и удобную схему представления оперативно-розыскной информации в виде таблиц, а также использование программных средств работы с данными, рассчитанных на неспециалистов в области программирования.

Вместе с тем, реляционная модель обладает рядом недостатков, которые приводят, на наш взгляд, к нецелесообразности ее использования для формирования массивов, подвергаемой аналитической обработке информации, получаемой и используемой в процессе оперативно-розыскной деятельности. На это указывают данные, полученные в ходе изучения практики использования подобных баз данных. К числу таких недостатков, по нашему мнению, можно отнести следующие.

---

[19] См., например: *Информатика* и математика для юристов: учебник для студентов вузов, обучающихся по юридическим специальностям / Под ред. С. Я. Казанцева и Н. М. Дубининой. – М., 2006. – С. 361-662.

[20] См., например: *Корнеев В. В.* Базы данных. Интеллектуальная обработка информации / В. В. Корнеев, А. Ф. Гареев, С. В. Васютин, В. В. Райх. – М., 2001. – С. 75.

[21] См.: *Барсегян А. А.* Методы и модели анализа данных: OLAP и Data Mining / А. А. Барсегян, М. С. Куприянов, В. В. Степаненко, И. И. Холод. – СПб., 2004. – С. 16.

[22] См.: *Роб П.* Системы баз данных: проектирование, реализация и управление / П. Роб, К. Коронел. – СПб., 2004. – С. 45.

[23] См.: См., например: *Барсегян А. А.* Методы и модели анализа данных: OLAP и Data Mining / А. А. Барсегян, М. С. Куприянов, В. В. Степаненко, И. И. Холод. – СПб., 2004. – С. 22-25.

[24] См.: См.: *Роб П.* Системы баз данных: проектирование, реализация и управление / П. Роб, К. Коронел. – СПб., 2004. – С. 72.

[25] См.: *Змитрович А. И.* Базы данных / А. И. Змитрович. – Минск, 1991. – С. 56-58.

Во-первых, это ее простота. Информация, подлежащая обработке и хранению, укладывается в плоские таблицы, в таких таблицах она структурирована. Однако в системах оперативно-розыскного назначения функционирует слабоструктурированная, нерегулярная информация. Отношения между такими таблицами не всегда адекватно отражает реальные информационные ситуации. Так, анализ дел оперативного учета, заведенных в оперативных подразделениях криминальной милиции, позволили выявить потребность в процессе оперативно-розыскной деятельности следующей информации, которую весьма затруднительно представить с использованием реляционной модели: привязку лица к нескольким адресам; связи между разрабатываемыми; использование автотранспортными средствами различными лицами и т.п.

Следующим недостатком реляционной модели представления данных, является то, что некоторые авторы определяют как достоинство – нормализация данных, их неделимость[26], в то время как при анализе в процессе осуществления оперативно-розыскной деятельности требуется представление описания лица, события или предмета в целом (агрегированная информация), либо представление отдельных характеристик объектов (детализированная информация). Так, изучение материалов дел оперативного учета, заведенных в оперативных подразделениях криминальной милиции, позволило выявить следующих характер обращений к имеющейся информации: требовалась агрегированная информация в 32 % случаев анализа; требовалась детализированная информация – в 68 %.

Существенным недостатком является и тот факт, что реляционная модель не предполагает существование хронологического порядка записей в таблицах, хотя некоторые виды анализа требуют упорядоченного во времени расположения данных. Из числа опрошенных нами сотрудников оперативных подразделений криминальной милиции 72,5 % отметили, что они в процессе анализа систематизировали имеющуюся информацию по времени происхождения событий.

Оценка уже имеющихся точек зрения на организацию массивов оперативно значимой информации позволяет выделить интересную, на наш взгляд, позицию Е. Г. Макарова и И. Л. Строгановой, которые, отмечая, что оперативно-розыскная деятельность представляет собой уникальную, трудно формализуемую предметную область, предлагают использование объектных систем управления базами данных, которые обеспечивают реализацию сетевой модели данных, либо наделение реляционных систем управления базами данных объектными свойствами.

Следует отметить, что сетевая модель разработана для того, чтобы более эффективно представлять сложные отношения данных. В настоящее время такая модель данных используется при построении баз данных в ряде подразделений оперативно-розыскной информации, а также в некоторых оперативных подразделениях криминальной милиции при формировании банков оперативно значимой информации.

К числу несомненных преимуществ данной модели представления данных следует отнести возможности описания связей "многие ко многим", а также автоматического выявления и представления опосредованных связей. Необходимо отметить, что потребность в выявлении связей довольно таки часто возникает в процессе решения задач оперативно-розыскной деятельности. Так, 87,5 %, опрошенных нами сотрудников оперативных подразделений криминальной милиции указали, что они подвергали дополнительной обработке (анализу) имевшуюся в наличии оперативно значимую информацию, осуществляя в 63,6 % случаев установление различных связей между лицами и фактами. Нам представляется необходимым указать на эффективность использования сетевой модели как средства реализации такого метода как построение диаграмм связей.

Наряду с имеющимися преимуществами сетевая модель обладает рядом недостатков. Так помимо недостатков, которые рассматриваются в литературе (сложность системы в целом и недостаточная структурная независимость[27]), на наш взгляд следует указать те, которые выявляются в процессе формирования массивов оперативно-розыскной информации и при ее анализе.

При формировании массивов оперативно-розыскной информации с использованием сетевой модели связи между отдельными объектами данных устанавливаются самим пользователем, а при осуществлении некоторых видов анализа осуществляется поиск связей. К тому же характер таких связей не всегда может быть определен однозначно. Так в 24,7 % случаев указание на характер связей в делах оперативно учета, заведенных в подразделениях криминальной милиции был предположительный. С использованием сетевой модели представления данных сложно определить связи неоднозначного характера. К тому же вновь, как и при использовании реляционной модели, мы можем столкнуться со сложностью представления данных в хронологическом порядке.

Отмеченные обстоятельства дают возможность нам сделать вывод о нецелесообразности использования реляционной и сетевой моделей для организации баз данных информационных систем, позволяющих осуществлять аналитическую обработку оперативно значимой информации в процессе оперативно-розыскной деятельности.

Наряду с реляционной и сетевой моделями, в научной литературе рассматриваются также иерархическая, объектно-ориентированная, многомерная модель "сущность-связь"[28]. Среди отмеченных, на наш взгляд, внимания заслуживает внимания многомерная модель представления данных, которая в настоящее

[26] См., например: *Кренке Д.* Теория и практика построения баз данных / Д. Кренке. – СПб., 2003. – С. 174.

[27] См., например: *Роб П.* Системы баз данных: проектирование, реализация и управление / П. Роб, К. Коронел. – СПб., 2004. – С. 56.

время уже начинает использоваться при построении информационных систем, реализующих аналитическую обработку[29]. К тому же, в числе правил интерактивной аналитической обработки, которые были сформулированы Э. Ф. Коддом, есть такое как многомерность концептуального представления данных[30].

Интерес к многомерной модели определяется такими ее достоинствами как более высокое, в сравнении с реляционными системами управления базами данных, быстродействие при ответе на сложные аналитические запросы, а также возможность решить задачу сложных нерегламентированных запросов[31].

Характеризуя многомерную модель представления данных, В. И. Ждамиров подчеркивает ее сущность – "не многомерность визуализации цифровых данных, а многомерное логическое представление структуры информации при описании и в операциях манипулирования данными"[32]. Основными понятиями многомерной модели являются измерение и значение. Измерение – это последовательность значений одного из анализируемых параметров. Измерения играют роль индексов, используемых для идентификации конкретных значений в ячейках гиперкуба пространства данных. Основные операции манипулирования измерениями (сечение, вращение, детализация и свертка) могут нами рассматриваться как аналитические операции.

Вместе с тем, нам представляется возможным именно с помощью многомерной модели фиксировать данные, которые имеют так называемые нечеткие значения, фактически устанавливая неявный характер связей между отдельными объектами, которые являются значениями измерений гиперкуба пространства данных.

Одним из наиболее важных достоинств многомерного представления оперативно-розыскной информации является возможность упорядоченного рассмотрения событий во времени, поскольку одним из измерений гиперкуба данных может быть время.

К приведенному выше следует добавить то, что решение задач, возникающих в процессе оперативно-розыскной деятельности, осуществляется, в том числе, путем анализа информации, образующей в своей совокупности многомерное информационное пространство. Именно пространство, а не информационное поле, как это утверждают некоторые авторы, под которым С. В. Лекарев и А. П. Судоплатов понимают идеальное бесконечномерное пространство, способное отобразить все состояние предметной области[33]. Реляционная модель только фиксирует координаты точек такого пространства. Сетевая модель отражает наличие известных связей между точками такого информационного пространства. Описывается такое пространство, по нашему мнению, многомерной моделью. Следует согласиться с мнением М. П. Малыхиной, утверждающей, что для человека, "занимающегося анализом данных, наиболее характерен многомерный взгляд на данные"[34].

Отмеченные обстоятельства позволяют нам сделать вывод о целесообразности использования многомерной модели при построении банков данных информационных систем, предназначенных для аналитической обработки оперативно-розыскной информации.

В целом же рассмотрение вопросов связанных с построением информационных систем, предназначенных для оперативных подразделений криминальной милиции.

Для обеспечения автоматизации аналитической обработки оперативно-розыскной информации в процессе осуществления оперативно-розыскной деятельности целесообразно использование специализированных информационных систем, реализующих методы интеллектуального анализа данных.

При формировании банков оперативно-розыскной информации информационных систем, предназначенных для оперативных подразделений криминальной милиции, необходимо использование многомерной модели представления данных.

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ДОКУМЕНТАЛЬНЫХ ПРОВЕРОК И РЕВИЗИЙ УПРАВЛЕНИЙ (ОТДЕЛОВ) ПО НАЛОГОВЫМ ПРЕСТУПЛЕНИЯМ МВД, ГУВД, УВД СУБЪЕКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

К.ю.н., доцент Н.Б. Егоров (Академия управления МВД России), к.ю.н.,. К.И. Гобрусенко (Федеральная служба по финансовому мониторингу)

Информатизация и компьютеризация управленческой и хозяйственной деятельности, транспорта, различных отраслей науки и производства открывают совершенно новые возможности по использованию современных информационных технологий в сфере борьбы с налоговой преступностью

[28] См., например: *Роб П.* Системы баз данных: проектирование, реализация и управление / П. Роб, К. Коронел. – СПб., 2004. – С. 45-70.

[29] См., например: *Филиппов В. А.* Многомерные СУБД при создании корпоративных информационных систем / В. А. Филиппов. – М., 2001; *Шекхар Ш.* Основы пространственных баз данных / Ш. Шекхар, С. Чаула – М., 2004.

[30] См.: *Филиппов В. А.* Многомерные СУБД при создании корпоративных информационных систем / В. А. Филиппов. – М., 2001. – С. 26.

[31] См.: *Малыхина М. П.* Базы данных: основы, проектирование, использование / М. П. Малыхина. – СПб., 2004.

[32] *Ждамиров В. И.* Основы информационных технологий: Учебное пособие / В. И. Ждамиров. – Воронеж, 2002. – с. 77.

[33] См.: *Судоплатов А. П.* Безопасность предпринимательской деятельности: Практическое пособие / А. П. Судоплатов, С. В. Лекарев. – М., 2001. – С. 271.

[34] *Малыхина М. П.* Базы данных: основы, проектирование, использование / М. П. Малыхина. – СПб, 2004. – С. 421.

Как показывает практика, в настоящее время успешно применяются разработанные на основе современных информационных технологий методики выявления налоговых преступлений и лиц их совершивших, а также получения сведений, необходимых для анализа и оценки оперативной обстановки. Данные методики могут также использоваться в рамках различных организационно-тактических форм оперативно-розыскной деятельности. Вместе с тем, мы полагаем, что современные информационные технологии можно успешно применять для документального оформления результатов проверочных мероприятий в отношении налогоплательщиков, осуществляемых подразделениями документальных проверок и ревизий управлений (отделов) по налоговым преступлениям МВД, ГУВД, УВД субъектов Российской Федерации.

В связи с компьютеризацией всех сфер человеческой деятельности значительная часть документов, отражающих финансово-хозяйственную деятельность налогоплательщиков, содержится в электронной форме. Бухгалтерский учет в кредитных организациях осуществляется в виде электронных баз данных, сформированных с использованием средств вычислительной техники. Формирование и ведение кредитной организацией электронной базы данных платежных документов и выписок по всем счетам закреплены ведомственными нормативными правовыми актами[1]. Кроме того, п. 2 ст. 80 Налогового кодекса Российской Федерации предусмотрел возможность поступления налоговых деклараций в электронной форме.

Проведенное нами исследование показало, что на основе современных информационных технологий можно разработать методику, которая позволит специалистам подразделений документальных проверок и ревизий на ранней стадии определить какая сумма денежной выручки за выполненные работы, отгруженную продукцию и т.д. в исследуемом периоде не поступила от различных хозяйствующих субъектов в кассу и на расчетные счета изучаемой организации, оценить на что данные денежные средства были использованы (на расширение материальной базы изучаемой организации, на непроизводственные нужды и т.д.).

В ст. 74 Уголовно-процессуального кодекса Российской Федерации[2] законодательно закреплено, что в качестве доказательств по уголовному делу выступают: с одной стороны, это любые сведения, а с другой – их процессуальные источники, к которым относятся заключения и показания специалиста, а также иные документы[3]. В ч. 2 ст. 84 УПК РФ содержание "иных документов" раскрывается следующим образом: "Документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, установленном статьей 86 настоящего Кодекса".

Акты ревизий и документальных проверок ранее применялись в доказывании как разновидность "иных документов"[4]. С введением изменений в УПК РФ заключение и показания специалиста является одним из процессуальных источников доказательств по уголовному делу[5]. Таким образом, акты документальных проверок и ревизий являются доказательством по уголовному делу. В соответствии с ч. 1 ст. 144 УПК РФ при проверке сообщения о преступлении орган дознания, следователь и прокурор вправе требовать производства документальных проверок, ревизий, привлекать к участию в них специалистов.

Документальные проверки, ревизии финансово-хозяйственной деятельности налогоплательщиков проводятся подразделениями документальных проверок и ревизий по первичным документам и сводным регистрам бухгалтерского и налогового учета (журналы-ордера ведомости, налоговые декларации, отчеты и т.д.) и по иным документам[6]. Результаты проведения проверок финансово-хозяйственной деятельности организаций отражаются в актах документальных проверок и ревизий, которые допускаются в качестве доказательств, как заключения специалиста.

Как показала практика, использование баз данных банковских учреждений позволяет быстро сформировать расчетную таблицу по использованию изучаемой организацией своих счетов и счетов третьих лиц для осуществления расчетов по ведению финансово-хозяйственной деятельности. После сравнения данных, содержащихся в сформированной таблице, с данными, отраженными в первичных документах,

---

[1] Об утверждении правил ведения бухгалтерского учета в кредитных организациях, расположенных на территории РФ, и дополнений и изменений к плану счетов бухгалтерского учета в кредитных организациях Российской Федерации// Приказ ЦБ РФ от 18.06.97 г. № 02-263 (с последующими изменениями и дополнениями); О порядке ведения кредитными организациями бухгалтерского учета и составления бухгалтерской отчетности в случае отключения информационных систем по задаче "Операционный день" (ручным способом)// Указание Центрального банка Российской Федерации от 22.12.99 г. № 706-У; Новый план счетов и правила ведения бухгалтерского учета в банках РФ в 1998 году// Предисловие Парфенова К.Г. – М.: ЗАО "Бухгалтерский бюллетень", 1997. С.9.

[2] Далее по тексту будет использоваться аббревиатура УПК РФ.

[3] Согласно ст. 5 Федерального закона от 29.12.94 г. № 77-ФЗ "Об обязательном экземпляре документов" (в ред. от 23.12.2003 г.) под документом понимается "материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи и изображения, предназначенный для передачи во времени и пространстве в целях их хранения и общественного использования".

[4] *Громов Н.А., Гущин А.Н., Луговец Н.В, Лямин М.В.* Доказательства, доказывание результатов оперативно-розыскной деятельности: Учебное пособие. – М.: "Приор-издат", 2005. – 160 с.

[5] См.: Федеральный закон от 04.07.2003 г. № 92-ФЗ "О внесении изменений и дополнений в Уголовно-процессуальный кодекс".

[6] Например, по журналам-ордерам № 6, № 8, № 9, № 11 и по ведомостям № 5 и 5-с (строительство).

сформированная таблица включается в акт документальной проверки, что позволяет существенно сокращать время написания акта документальной проверки, в особенности при проверки крупных налогоплательщиков.

Таким образом, для анализа финансово-хозяйственной деятельности налогоплательщика, мест нахождения документов, ее отражающих, а также установления его контрагентов необходимо использовать электронные копии баз данных платежных документов коммерческих банков, где открыты лицевые счета налогоплательщика, и расчетного кассового центра (РКЦ) территориального учреждения Банка России, т.е. использовать базы данных "Банки". Для этого по банковским счетам из базы данных необходимо выбрать следующие сведения расчетных документов: "Дата", "Сумма операции", "Назначение платежа", "БИК (Банковский идентификационный код) банка плательщика", "Номер лицевого счета плательщика", "Наименование плательщика", "ИНН плательщика", "БИК банка получателя", "Номер лицевого счета получателя", "Наименование получателя", "ИНН получателя".

В качестве критерия поиска в запросе по полю "Номер лицевого счета плательщика" указывается номер каждого лицевого счета налогоплательщика, а по полю "БИК плательщика" соответствующий банковский идентификационный код банка, в котором открыт счет налогоплательщика. Также в качестве критерия поиска в запросе по полю "ИНН плательщика" можно указать ИНН организации. Таким образом, устанавливаются все расходные операции налогоплательщика, что позволяет сформировать следующую таблицу.

Дата	Сумма	Назначение платежа	БИК плательщика	Счет плательщика	ИНН плательщика	Наименование плательщика	БИК получателя	Счет получателя	ИНН получат.	Наименование получателя

Для установления документов, на основании которых осуществлялось поступление и расходование денежных средств по расчетным счетам хозяйствующих субъектов за рассматриваемый период, запросы формируются по полям: "Номер лицевого счета плательщика", "БИК плательщика", либо "ИНН плательщика" и "Номер лицевого счета получателя", "БИК получателя", либо "ИНН получателя".

По базам данных РКЦ территориального учреждения Банка России устанавливается: предъявлялись ли в банк денежные средства по расчетным документам со счетов исследуемой организации для перечисления в бюджеты разных уровней (на уменьшение недоимки) и в государственные внебюджетные фонды (на погашение задолженности). Если же денежные средства исследуемой организации перечислялись в бюджеты разных уровней и в государственные внебюджетные фонды, то устанавливается какие суммы поступили за рассматриваемый период и на основании каких документов.

Таким образом, по полю "Назначение платежа" баз данных банковского учреждения или РКЦ территориального учреждения Банка России устанавливаются места нахождения расчетных документов, используемых при безналичных расчетах: платежные поручения, аккредитивы, чеки, платежные требования, инкассовые поручения.

По сформированной таблице ответа проводится анализ на основании каких финансово-хозяйственных документов осуществлялось движение денежных средств по банковским счетам проверяемого налогоплательщика в части их поступления и расходования, а также устанавливаются места возможного нахождения этих документов.

На основе этой таблицы осуществляется отбор финансовых операций для сверки с данными по первичным документам, с помощью ЭВМ формируется окончательная таблица, которая включается в акт проверки.

Плательщик	Получатель	№ платежного поручения	Дата	Назначение платежа	Сумма, руб.

Документы, на основании которых осуществляется финансово-хозяйственная деятельность налогоплательщиков по взаимозачетной схеме и через счета 3-х лиц, и места их нахождения, а также контрагенты устанавливаются аналогичным образом по сведениям, содержащихся в расчетных документах в разделе "Назначение платежа", который в базах данных банковских учреждений и РКЦ территориального учреждения Банка России выделен отдельным полем.

Резюмируя сказанное, можно сделать вывод, что использование подразделениями документальных проверок и ревизий Управлений (отделов) по налоговым преступлениям МВД, ГУВД, УВД предложенной нами методики позволит им снизить трудоемкость обработки первичных документов и сократить время проведения проверочных мероприятий в отношении налогоплательщиков и подготавливаемых по их результатам актов.

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ – КАК УГРОЗА ЭКОНОМИЧЕСКОЙ И ИНФОРМАЦИОННОЙ СФЕРАМ

А.В. Ежеватов (Академия управления МВД России)

Человеческое общество в своем развитии прошло несколько этапов. На каждом этапе основой социальных отношений в обществе являлась экономика. Рабовладельческий строй, сменил феодальный, феодальный - капитализм. Капитализм начала 20 века существенно отличается от капитализма начала века 21. На смену индустриальной экономике приходит "экономика знаний", создающая условия, при которых инвестирование осуществляется в новые знания, в дальнейшем обеспечивающие основную норму прибыли. В рамках данной модели создаются новые базовые продукты, требующие для своего производства новые технологические процессы и новое технологическое оборудование. Всё это стало возможным благодаря развитию в конце 20 века компьютерных технологий, которые играют ключевую роль в развитии человеческих знаний. Без них не обходится ни одна значимая область человеческой деятельности.

Но опыт человечества показывает, что у любого явления существует обратная сторона. Открытие в 20 веке расщепления атома послужило основой, как для создания атомных электростанций, так и для создания атомной бомбы. Точно также и с современными компьютерными технологиями. С одной стороны, благодаря им, происходит ускорение всех социальных процессов - мир становиться безопаснее и открытие, удобнее и комфортнее. С другой стороны, последствия от неправильного функционирования компьютерных систем создают существенную угрозу человеку, обществу и государству. Данная проблема в настоящее время является актуальной и для современной России.

Специалисты по национальной безопасности классифицируют угрозы на внешние и внутренние, угрозы политические, экономические, военные, информационные и т.д. В "Концепции национальной безопасности Российской Федерации"[35] были определены первостепенные угрозы национальной безопасности. В настоящей статье остановимся на угрозах в экономической и информационной сферах более подробно.

Основными условиями угроз:

в сфере экономики определены - ослабление научно-технического и технологического потенциала страны; сокращение исследований на стратегически важных направлениях научно-технического развития; отток за рубеж специалистов и интеллектуальной собственности; снижение инвестиционной, инновационной активности и научно-технического потенциала;

в информационной сфере - стремление ряда стран к доминированию в мировом информационном пространстве, способствующие вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Из стоящих перед органами государственной власти Российской Федерации задач обеспечения экономической и информационной безопасности хотелось бы выделить задачи, напрямую решаемые органами внутренних дел.

К общим задачам относятся:

1. своевременное прогнозирование и выявление внешних и внутренних угроз национальной безопасности Российской Федерации;
2. реализация оперативных и долгосрочных мер по предупреждению и нейтрализации внутренних и внешних угроз;
3. обеспечение на территории России личной безопасности человека и гражданина, его конституционных прав и свобод;
4. совершенствование системы государственной власти Российской Федерации, федеративных отношений, местного самоуправления и законодательства Российской Федерации, формирование гармоничных межнациональных отношений, укрепление правопорядка и сохранение социально-политической стабильности общества;
5. обеспечение неукоснительного соблюдения законодательства Российской Федерации всеми гражданами, должностными лицами, государственными органами, политическими партиями, общественными и религиозными организациями.

К задачам в сфере экономики:

1. совершенствование экономических отношений в сфере валютного регулирования и контроля в целях создания условий для прекращения расчетов в иностранной валюте на внутреннем рынке и предотвращения бесконтрольного вывоза капитала;
2. правовое обеспечение экономических реформ и создание эффективного механизма контроля за соблюдением законодательства Российской Федерации;
3. усиление государственной поддержки инвестиционной и инновационной активности, принятие мер по созданию устойчивой банковской системы, отвечающей интересам реальной экономики, облегчение доступа предприятий к долгосрочным кредитам на финансирование капитальных вложений;

[35] Концепция национальной безопасности Российской Федерации утверждена Указом Президента Российской Федерации от 17 декабря 1997 года № 1300 (В редакции утвержденной Указом Президента Российской Федерации от 10 января 2000 года № 24).

4. защита интеллектуальной собственности внутри страны и за рубежом;
5. содействие созданию равных условий для развития и увеличения конкурентоспособности предприятий независимо от формы собственности, в том числе становлению и развитию частного предпринимательства во всех сферах, где это способствует росту общественного благосостояния, прогрессу науки и образования, духовному и нравственному развитию общества, защите прав потребителей.

К задачам в информационной сфере:

1. реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;
2. совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
3. противодействие угрозе развязывания противоборства в информационной сфере.

Кроме вышеназванных задач обеспечения безопасности Российской Федерации в сфере экономики и информационной сфере, органы внутренних дел решают следующие задачи в области борьбы с преступностью:

1. выявление, устранение и предупреждение причин и условий, порождающих преступность;
2. усиление роли государства как гаранта безопасности личности и общества, создание необходимой для этого правовой базы и механизма ее применения;
3. укрепление системы правоохранительных органов, прежде всего структур, противодействующих организованной преступности и терроризму, создание условий для их эффективной деятельности;
4. привлечение государственных органов в пределах их компетенции к деятельности по предупреждению противоправных деяний;
5. расширение взаимовыгодного международного сотрудничества в правоохранительной сфере, в первую очередь с государствами - участниками Содружества Независимых Государств.

Проанализировав задачи обеспечения безопасности в сфере экономики и информационной сфере, стоящие перед органами внутренних дел, можно выделить два взаимосвязанных элемента:

- современным экономическим и информационным сферам для нормального развития требуется использование современных компьютерных технологий;

- государство создает эффективный механизм обеспечения безопасности используемых компьютерных технологий, осуществляет мониторинг происходящих процессов в этой области, обеспечивает защиту имеющимися средствами: правовыми, организационными, техническими и т.д.

Одним из важных элементов механизма обеспечения безопасности является уголовно-правовая охрана общественных отношений в экономической и информационной сферах. Одним из видов преступлений, затрагивающих охраняемые уголовным законом общественные отношения в обеих сферах, выступают преступления, совершаемые с использованием компьютерных технологий - так называемая "компьютерная преступность". Различные специалисты наполняют понятие "компьютерная преступность" разным содержанием. Существуют такие подходы:

1. Закрепленное в Уголовном Кодексе РФ понятие "преступления в сфере компьютерной информации"[36] в статьях:
   - ст. 272. "Неправомерный доступ к компьютерной информации";
   - ст. 273. "Создание, использование и распространение вредоносных программ для ЭВМ";
   - ст. 274. "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети".
2. "Преступления, сопряженные с использованием компьютерных средств" - кроме преступлений, предусмотренных в главе 28 УК РФ, предлагается[37] отнести к данному виду следующие составы преступлений:
   - ст. 146. "Нарушение авторских и смежных прав (в части защиты авторских прав на программы для ЭВМ и базы данных);
   - ст. 159. "Мошенничество";
   - ст. 165. "Причинение имущественного ущерба путем обмана или злоупотребления доверием";
   - ст. 187. "Изготовление и сбыт поддельных кредитных либо расчетных карт и иных платежных документов";
   - ст. 292. "Служебный подлог";
   - ст. 174. "Легализация (отмывание) денежных средств или иного имущества, приобретенного незаконным путем (в случае, если преступник перевел деньги со счета зарубежного банка на свой счет в российском банке и получает по этому вкладу начисляемые проценты";
   - ст. 183. "Незаконное получение или разглашение сведений, составляющих коммерческую или банковскую тайну (здесь под категорию коммерческой тайны подпадает список пользователей компьютерной системы с их паролями)";

[36] Уголовный кодекс Российской федерации. Глава 28.

[37] Е.Л. Логинов. Отмывание денег через Интернет - технологии. М. 2005 г. стр. 115

- ст. 129. "Клевета" (в случае размещения в сети Интернет заведомо ложных сведений, порочащих честь и достоинство определенного лица);
- ст. 137. "Нарушение неприкосновенности частной жизни" (при размещении в сети Интернет информации, которая относится к категории личной и или семейной тайны);
- ст. 138. "Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений" (здесь речь идет об уголовной ответственности за чтение чужих электронных писем).

3. "Телекоммуникационное мошенничество" - неправомерная деятельность, связанная с несанкционированным пользованием услугами связи.[38]
4. "Компьютерное преступление" - предусмотренное уголовным законом общественно опасное деяние (действие или бездействие), направленное против информации, представленной в особом (машинном) виде, принадлежащей государству, юридическому или физическому лицу, а также против установленного государством или ее собственником порядка создания (приобретения), использования и уничтожения, если оно причинило или представляло реальную угрозу причинения ущерба законному владельцу информации или автоматизированной системы, в которой эта информация генерируется (создается), обрабатывается, передается и уничтожается, или повлекло иные опасные последствия.[39]
5. "Безопасность в области высоких технологий" - видовой объект преступлений, к которому относят: ч. 2 ст. 138. "Нарушение тайны переписки, телефонных переговоров, телеграфных и иных сообщений с использованием специальных технических средств, предназначенных для негласного получения информации"; ч. 3 ст. 138. "Незаконный сбыт или приобретение в целях сбыта таких средств"; ст. 189. "Незаконный экспорт технологий, научно-технической информации и услуг, используемых при создании оружия массового поражения, вооружения и военной техники", преступления, предусмотренные гл. 28 УК РФ.[40]

Проблема борьбы с преступлениями, совершаемыми с использованием компьютерных технологий актуальны не только для нашей страны, данные преступления - наднациональные. Они создают угрозу нормальному функционированию экономической и информационной сфер всех стран. Поэтому данные проблемы рассматриваются на самом высоком межгосударственном уровне. Результатом такого взаимодействия является принятие важных документов - источников международного права в сфере борьбы с "компьютерной преступностью". К ним относятся следующие документы:

- "Соглашение о борьбе с распространением порнографических изданий", подписанное в Париже 4 мая 1910 года, с изменениями, внесенными протоколом, подписанным в Лейк Соксес, Нью-Йорк, 4 мая 1949 года;
- "Конвенция Организации Объединенных Наций против транснациональной организованной преступности", принятая резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года;
- "Окинавская хартия Глобального информационного общества (Okinava Charter)", принятая 22 июля 2000 года лидерами стран "Большой восьмерки".

Также необходимо выделить самый авторитетный в настоящее время международный документ в сфере борьбы с "компьютерной преступностью" - Международную "Конвенцию о киберпреступности", принятую в Будапеште 23 ноября 2001 года государствами членами Совета Европы и вступившую в силу в июле 2004 года. Данная конвенция имеет открытый характер, любая страна может подать заявку на присоединение к ней. По состоянию на 2006 год конвенцию подписали 45 стран, из которых в течение 6 лет в 18 странах её ратифицировали. Последней из стран, присоединившихся к международной конвенции, являются США, подавшие заявку на участие с 1 января 2007 года. Россия не входит в число стран, присоединившихся к конвенции. Основным принципиальным противоречием является содержание главы 32 "Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным". Ее неясная формулировка позволяет осуществлять проникновение в информационные сети другого государства без его уведомления, опираясь на чье-то разрешение.[41]

Данная конвенция предлагает странам-участницам принять уголовно-правовые меры на национальном уровне в целях эффективной международной борьбы с компьютерными преступлениями. Данные меры касаются как уголовного, так и уголовно-процессуального права. В конвенции предложено закрепить

[38] Г.В. Семенов. Телекоммуникационное мошенничество: введение в проблему // Воронежские криминалистические чтения. Вып. 1 / Под ред. О.Я. Баева. – Воронеж: Издательство Воронежского государственного университета, 2000 г. – С. 100 – 106.

[39] В.А. Мещеряков. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. Воронеж: ВГУ. 2001 г.

[40] С.Г. Спирина. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации. Автореферат на соискание ученой степени кандидата юридических наук. Волгоград. 2001 г.

[41] Выступление начальника Бюро специальных технических мероприятий МВД России генерал-полковника милиции Бориса Мирошникова на конференции в рамках Проекта Международного сотрудничества по уголовным делам на тему: "Перспективы международного сотрудничества в рамках Конвенции о киберпреступности 2001 г.". 6 февраля 2007 года, Киев. http://www.mvd.ru/press/interview/4625/

уголовную ответственность за следующие преступления:

Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

1.**Противозаконный доступ** - доступ, когда он является преднамеренным, к компьютерной системе в целом или любой ее части без права на это.

2.**Противозаконный перехват** - преднамеренно осуществленный с использованием технических средств перехват - без права на это - не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные.

3.**Воздействие на данные** - преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных без права на это.

4.**Воздействие на функционирование системы -** преднамеренное создание - без права на это - серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.

5.**Противозаконное использование устройств** - нижеследующие деяния в случае их совершения преднамеренно и без права на это: производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование: устройств, включая компьютерные программы, разработанные или адаптированные прежде всего для целей совершения какого-либо из правонарушений, предусмотренных выше в статьях; компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части с намерением использовать их для совершения какого-либо из правонарушений, предусмотренных в статьях; владение одним из предметов, упомянутых выше, с намерением использовать его для совершения каких-либо правонарушений, предусмотренных выше в статьях.

Правонарушения, связанные с использованием компьютерных средств:

6.**Подлог с использованием компьютерных технологий -** ввод, изменение, стирание или блокирование компьютерных данных, влекущих за собой нарушение аутентичности данных с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными.

7.**Мошенничество с использованием компьютерных технологий** - лишение другого лица его собственности путем: любого ввода, изменения, удаления или блокирования компьютерных данных; любого вмешательства в функционирование компьютерной системы, с мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.

Правонарушения, связанные с содержанием данных:

8.**Правонарушения, связанные с детской порнографией** – совершение, преднамеренно и без права на это, следующих деяний: производство детской порнографической продукции с целью распространения через компьютерную систему; предложение или предоставление в пользование детской порнографии через компьютерную систему; распространение или передача детской порнографии через компьютерную систему; приобретение детской порнографии через компьютерную систему для себя или для другого лица; владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных.

Правонарушения, связанные с нарушением авторского права и смежных прав:

9.**Правонарушения, связанные с нарушением авторского права и смежных прав** - действия, совершаемые преднамеренно в коммерческом масштабе и с помощью компьютерной системы, за исключением любых моральных прав, предоставляемых Парижской конвенцией от 24 июля 1971 года, об охране литературных и художественных произведений, по Соглашению о торговых аспектах прав интеллектуальной собственности и по Договору об авторском праве Всемирной организации интеллектуальной собственности (ВОИС).[42]

Несмотря на достаточно небольшое время, прошедшее с момента принятия конвенции, уже имеются факты иных видов преступлений, совершаемых с использованием компьютерных технологий, не предусмотренных в её тексте. Например: вымогательство, преступлений против правосудия.

Закрепляемые в уголовно-процессуальном праве условия и гарантии реализации положений конвенции:

1.**Оперативное обеспечение сохранности хранимых компьютерных данных**, включая данные о потоках информации, которые хранятся в компьютерной системе, в частности, когда имеются основания полагать, что эти компьютерные данные особенно подвержены риску утраты или изменения. Должны реализовываться следующие требования: хранить компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего 90 дней, чтобы компетентные органы могли добиться раскрытия этих компьютерных данных; обязать хранителя или другое лицо, которому поручено обеспечивать сохранность компьютерных данных, сохранять конфиденциальность выполнения таких процедур

[42] Международная "Конвенция о киберпреступности", принятая в Будапеште 23 ноября 2001 года государствами членами Совета Европы.

в течение срока, предусмотренного ее внутригосударственным правом.

2.**Оперативное обеспечение сохранности и частичное раскрытие данных о потоках информации** - гарантии: обеспечение сохранности данных о потоках информации было возможным независимо от того, сколько поставщиков услуг были вовлечены в передачу соответствующего сообщения - один или более; оперативное раскрытие компетентным органам этой Стороны или лицу, назначенному этими органами, достаточного количества данных о потоках информации, которое позволит соответствующей Стороне идентифицировать поставщиков услуг и путь, которым передавалось данное сообщение.

3.**Распоряжение о предъявлении** - предоставление ее компетентным органам полномочия отдавать распоряжения:

- о предъявлении конкретных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на том или ином носителе компьютерных данных; поставщику услуг, предлагающему свои услуги на ее территории,
- о предъявлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах.

4.**Обыск и выемка хранимых компьютерных данных** - предоставление ее компетентным органам полномочий на обыск или иной аналогичный доступ к: компьютерным системам или их частям, а также хранящимся в них компьютерным данным; носителям компьютерных данных, на которых могут храниться искомые компьютерные данные, на ее территории.

5.**Сбор и перехват компьютерных данных в режиме реального времени** - предоставление ее компетентным органам полномочий: собирать или записывать с применением технических средств на территории этой Стороны; заставлять поставщиков услуг, в пределах имеющихся у них технических возможностей, собирать или записывать с применением технических средств на территории этой Стороны; сотрудничать с компетентными органами и помогать им в сборе или записи в реальном масштабе времени данных о потоках информации, связанных с конкретными сообщениями на территории этой Стороны, передаваемыми по компьютерной системе.

Небольшой анализ приведенных уголовно-процессуальных норм позволяет сделать вывод о наличии в них норм регламентирующих оперативно-розыскную деятельность (абзац 5). Провести полный анализ оперативно-розыскных деятельности по борьбе с преступлениями, совершаемыми с использованием компьютерных технологий в различных странах невозможно, учитывая специфичный (закрытый характер) такой деятельности. Но, используя открытые источники информации, можно выделить элементы нормативно-правового, организационно-структурного обеспечения, определить ряд проводимых оперативно-розыскных мероприятий и действий, способствующих, так или иначе, решению задач оперативно-розыскной деятельности. Рассмотрим это на примере деятельности следующих стран:

Великобритания

В системе министерства внутренних дел Великобритании в 2001 году создано полицейское подразделение по борьбе с киберпреступностью - "Национальное подразделение по борьбе с преступлениями в сфере высоких технологий" (National High Tech Crime Unit - NHTCU). Основной функцией NHTCU является борьба с организованной киберпреступностью, под которой подразумевается хакерство, приравненное британским законодательством к терроризму, и различные финансовые мошенничества с использованием высоких технологий. Одной из мер, позволяющих эффективно бороться с киберпреступностью, предлагается принятие новых законов. В частности, полиция предлагает ввести закон, согласно которому весь трафик, идущий на Великобританию, сохранялся бы в течение 5 лет. Обязанность по хранению трафика, под которым подразумевается, прежде всего, электронная почта, будет возложена на провайдеров.

В октябре 2000 года британское правительство обнародовало правила, согласно которым компании-работодатели получили право на прослушивание телефонных разговоров и просмотр электронной почты своих сотрудников. Данные правила являются частью закона RIP (Regulations of Investigatory Powers), который также устанавливает слежку за трафиком интернет-провайдеров, обязывает всех граждан предоставлять компетентным органам любые пароли или криптографические ключи.

Соединенные Штаты Америки

В 1986 конгресс США принят "Акт о компьютерном мошенничестве и злоупотреблениях". Причиной этому, в частности, послужили действия Иана Мерфи, также известного как Captain Zap, который взламывал военные компьютеры, похищал информацию из базы данных заказов компаний и звонил по телефону через правительственные каналы связи. На основании данного нормативно-правового акта было создано подразделение ФБР по борьбе с компьютерными преступлениями.

В 1999 году был создан единый координирующий орган, занимающийся борьбой с компьютерной преступностью на всей территории страны. До этого граждане США могли подавать жалобы в местное полицейское управление, ФБР и другие федеральные правоохранительные органы, Федеральную комиссию по торговле или Почтовую инспекционную службу США (правоохранительное подразделение Почтовой службы США). Созданный в городе Моргантаун, штат Западная Вирджиния, Центр стал занимаеться рассмотрением жалоб о мошенничестве в Интернете. Его деятельность осуществлялась в партнерстве с ФБР и Национальным центром по борьбе с преступностью "белых воротничков". Это была некоммерческая структура, которая действовала под эгидой Министерства юстиции США, главная цель которой состояла в укреплении потенциала штатских и местных правоохранительных органов в выявлении и пресечении экономических преступлений и

компьютерных преступлений. В 2002 году, после уточнения определения киберпреступности, которая стала охватывать преступления, начиная от обычного мошенничества и кончая правонарушениями в режиме онлайн, единый координирующий орган был переименован в Центр рассмотрения жалоб на противозаконные действия в Интернете. И ФБР обратилось с призывом к другим федеральным структурам, таким как Почтовая инспекционная служба США, Федеральная комиссия по торговле, Секретная служба, помочь с комплектованием центра специалистами и поддержать его усилия по борьбе с киберпреступностью.

Сегодня в Центре рассмотрения жалоб на противозаконные действия в Интернете находится в городе Фэрмонт, штат Западная Вирджиния. В нём работают шесть федеральных агентов и около 40 аналитиков из промышленных фирм и университетов, которые принимают от граждан жалобы о правонарушениях в Интернете, изучают их и направляют в соответствующие федеральные, штатские, местные или международные правоохранительные или регулирующие органы, а также специальные межведомственные группы для проведения расследований. Как видно, данный орган выполняет координирующие функции в борьбе с компьютерными преступлениями не только на территории США но и за её пределами.

Республика Беларусь

В системе МВД созданы специализированные оперативно-розыскные подразделения по борьбе с компьютерными преступлениями. В настоящее время эти задачи решаются управлением по раскрытию преступлений в сфере высоких технологий МВД и его подразделениями на местах. Кроме того, в 2006 г. в структуре Главного управления предварительного расследования МВД было создано управление по расследованию преступлений в сфере высоких технологий и интеллектуальной собственности.

Российская Федерация

14 августа 1998 года было создано Управление по борьбе с преступлениями в сфере высоких технологий МВД Российской Федерации, которые, после проведенной реорганизации в декабре 2001 года, стали называться подразделениями по борьбе с компьютерными преступления и незаконным оборотом радиоэлектронных средств и специальных технических средств (подразделениями "К") ОВД Российской Федерации.

Основными направлениями деятельности являются: борьба с преступлениями в компьютерной сфере - объектом преступного посягательства является информация находящаяся в ЭВМ, а также информация, передаваемая по телекоммуникационным сетям; пресечение оборота контрафактной аудио-, видеопродукции и программного обеспечения; борьба с незаконным оборотом радиоэлектронных и специальных технических средств (СТС); борьба с преступлениями в сфере использования электронных платежных карт и систем электронных платежей в сети Интернет; борьба с преступлениями в сфере телекоммуникаций.

Правовую основу деятельности Управления составляют: Конституция Российской Федерации; Закон Российской Федерации "О милиции"; Федеральный Закон Российской Федерации "Об оперативно-розыскной деятельности"; Закон Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных"; Федеральный закон "Об информации, информатизации и защите информации"; Федеральный закон "О связи"; Федеральный закон "Об авторском праве и смежных правах"; "Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность", утвержденные постановлением Правительства РФ № 538 от 27.08.2005 г., и др.

По данным Управления "К" БСТМ МВД России в 2004 году зарегистрировано 13 261 преступление, в 2005 - 14 810, в 2006 - чуть более 14 000.[43] Но в тоже время отмечается качественное изменение совершаемых преступлений в сторону увеличения наносимого ущерба. Половина зафиксированных преступлений относится к несанкционированному доступу к компьютерной информации. Растет корыстная направленность компьютерных преступлений вместе с нанесенным материальным ущербом. Растет количество преступлений, совершенных группами. Растет количество трансграничных компьютерных преступлений. По-прежнему высока латентность компьютерной преступности.[44]

Подводя итоги, необходимо сделать следующие выводы.

При расследовании преступлений, совершаемых с использованием компьютерных технологий, успех зависит от сочетания новых и классических методов раскрытия.

Как правило, компьютерные преступления становятся лишь первым шагом в цепочке криминальных деяний, направленных на другие традиционные преступления - хищения, вымогательства, мошенничества и так далее.

Учитывая трансграничный характер совершаемых преступлений, анонимность, высокие скорости процессов, эффективная борьба с преступлениями, совершаемыми с использованием компьютерных технологий, возможна лишь при тесном взаимодействии правоохранительных органов с государственным и частным сектором, а также налаженное взаимодействие с правоохранительными органами иностранных государств и международными организациями.

По мнению ряда экспертов, серьезная работа должна быть проведена по совершенствованию оперативно-розыскного законодательства в части:

[43] См. Выступление Мирошникова Б.Н. http://www.mvd.ru/press/interview/4625/

[44] См. Выступление Мирошникова Б.Н. http://www.mvd.ru/press/interview/4625/

- создания необходимых условий для проведения оперативно-розыскных мероприятий в целях выявления, предупреждения, пресечения и раскрытия компьютерных преступлений и преступлений в сфере высоких технологий;
- усиления контроля за сбором, хранением и использованием информации о частной жизни граждан, сведений, составляющих личную, семейную, служебную и коммерческую тайны;
- уточнения состава оперативно-розыскных мероприятий.[45]

Повышение уровня профессиональной подготовки сотрудников правоохранительных органов так или иначе связанных с выявлением, раскрытием и расследованием компьютерных преступлений.

Налаживание международного сотрудничества в разработке судебных стандартов поиска и установление подлинности электронных данных.

ВОПРОСЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО СОВЕРШЕНСТВОВАНИЯ УЧЕТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА ПРИМЕРЕ СТАТИСТИКИ В СФЕРЕ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА

А.А. Кузнецов (Академия управления МВД России)

Автоматизированная статистическая отчетность в системе органов внутренних дел имеет огромное значение не только в силу необходимости проведения объективного анализа результатов оперативно-розыскной деятельности, но и для выработки стратегических решений по борьбе с преступностью, в том числе и в сфере экономики. В ряде случаев это напрямую связано с необходимостью увеличения штатной численности ряда структурных подразделений, целесообразностью создания дополнительных оперативно-розыскных бюро, отделений, отделов по направлениям деятельности и рядом других подобных вопросов.

Нельзя не отметить тот факт, что несовершенство статистических учетов МВД России уже нередко негативно освещается и в средствах массовой информации, что серьезно подрывает престиж органов внутренних дел в целом.

Например, в газете "Ведомости" № 48 (1822) от 20 марта 2007 года журналист Анастасия Корня в своей статье "Ущербная отчетность" указывает на то, что "…ущерб от экономических преступлений в прошлом году по данным МВД, упал более чем в 10 раз по сравнению с позапрошлым, хотя количество самих преступлений этого рода выросло на 11,8 %. Аномальный прирост ущерба от экономической преступности в 2005 г. – до 1,4 трлн. руб.! – эксперты объясняют и кампанией по борьбе с незаконным предпринимательством, и делом ЮКОСа, и приписками в статистике, и коррупцией…". По словам адвоката Игоря Трунова, также упоминающегося в данной статье, "…цифры из статистики МВД просто надуманы, именно поэтому их колебания столь грандиозны...", "…судебная практика показывает, что в рамках уголовных дел случаи возмещения ущерба потерпевшим носят единичный характер, что и свидетельствует о реальной картине с выявлением нанесенного преступниками ущерба…" - считает Трунов.

Рассматривая данный вопрос по существу мы увидим, что обвинения в адрес МВД России беспочвенны, а возникшие у журналиста А. Корня и адвоката И. Трунова вопроса связаны не только с их некомпетентностью, но и с несовершенством действующей в МВД России системы статистической отчетности.

Обращаясь к статистике мы видим, что по данным ГИАЦ МВД России в 2006 году правоохранительными органами Российской Федерации всего выявлено 489 554 преступления экономической направленности (+ 11,8 %), в том числе следствие по которым обязательно – 311 135 преступлений (+ 14,1 %).

В 2005 году общий размер установленного материального ущерба на момент возбуждения уголовных дел о преступлениях экономической направленности составил 1399,6 млрд. рублей, в том числе на момент возбуждения уголовных дел о преступлениях следствие по которым обязательно – 1388,5 млрд. рублей.

В 2006 году общий размер установленного материального ущерба по оконченным расследованием уголовным делам составил 127,5 млрд. рублей, в том числе по оконченным уголовным делам следствие по которым обязательно – 123,4 млрд. рублей.

Подразделениями по борьбе с экономическими преступлениями в 2006 году выявлено 226 117 преступлений (+ 12,4 %), в том числе следствие по которым обязательно – 205 931 преступление (+ 14,9 %).

В 2005 году по лини работы подразделений БЭП общий размер установленного материального ущерба на момент возбуждения уголовных дел составил 635,7 млрд. рублей, в том числе на момент возбуждения уголовных дел о преступлениях следствие по которым обязательно – 632 млрд. рублей.

[45] В.А.Васильев, Председатель Комитета по безопасности Государственной Думы РФ, "Проблемы развития законодательства в сфере борьбы с киберпреступностью", Международная практическая конференция по борьбе с киберпреступностью и кибертерроризмом, 19-20 апреля 2006 г., Москва

В 2006 году общий размер установленного материального ущерба по оконченным уголовным делам составил 49,3 млрд. рублей, в том числе по оконченным уголовным делам следствие по которым обязательно – 48,2 млрд. рублей.

Подразделениями по налоговым преступлениям в 2006 году выявлено 25 623 преступления (+ 12,3 %), в том числе следствие по которым обязательно – 24 309 преступлений (+ 15,1 %).

В 2005 году по лини работы подразделений НП общий размер установленного материального ущерба на момент возбуждения уголовных дел составил 711,5 млрд. рублей, в том числе на момент возбуждения уголовных дел о преступлениях следствие по которым обязательно – 710,4 млрд. рублей.

В 2006 году общий размер установленного материального ущерба по оконченным уголовным делам составил 56,8 млрд. рублей, в том числе по оконченным уголовным делам следствие по которым обязательно – 56,6 млрд. рублей.

Показатели размера установленного материального ущерба в 2005 году и в 2006 году не подлежат сравнению, поскольку в 2006 году произошло принципиальное изменение раздела 4 (правоохранительные органы), раздела 5 (подразделения НП) и раздела 15 (подразделения БЭП) формы 1А. В соответствии с изменениями, внесенными в статистическую отчетность ГИАЦ МВД России, с 01 января 2006 года сумма установленного материального ущерба как в целом, так и отдельно по отраслям народного хозяйства, исчисляется по оконченным расследованием уголовным делам, в то время как в 2005 году данный показатель исчислялся на момент возбуждения уголовных дел.

В соответствии со статистической отчетностью, наглядно свидетельствующей о количестве выявленных преступлений в сфере топливно-энергетического комплекса (ТЭК), подразделениями по борьбе
с экономическими преступлениями по итогам 2006 года в сравнении с 2005 годом имеются существенные различия.

Так, в 2005 году подразделениями БЭП на территории России по линии ТЭК выявлено 7 726 преступлений. Размер установленного материального ущерба на момент возбуждения уголовных дел составил 588,9 млрд. рублей.

По итогам 2006 года подразделениями БЭП субъектов Российской Федерации по линии ТЭК выявлено 7 286 преступлений (меньше в 1,06 раза), а размер установленного ущерба по оконченным расследованием уголовным делам составил 2,3 млрд. рублей.

Таким образом, мы видим, что различие в размере материального ущерба по оконченным расследованием уголовным делам и на момент возбуждения уголовных дел существенное, но, как упоминалось выше, они не подлежат сравнению.

Как известно, сфера ТЭК состоит из следующих подразделов:

- нефтедобыча, переработка и реализация нефтепродуктов;
- химическая и нефтехимическая промышленность;
- добыча, переработка, транспортировка и реализация газа;
- недропользование;
- электроэнергетика;
- горнодобывающая и угольная промышленность.

В связи с несовершенством действующей в МВД России системы отчетности, не представляется возможным провести анализ статистических данных о количестве выявленных преступлений и размере причиненного ущерба. На примере указанных подразделов, в том числе с участием подразделений по налоговым преступлениям, чья роль в выявлении преступлений экономической направленности в сфере ТЭК немаловажна, поскольку действующая статистическая отчетность ГИАЦ МВД России (форма 1А) не предусматривает учета количества преступлений и размера установленного материального ущерба в сфере ТЭК как по каждому из подразделов, так и с участием подразделений НП, что также относится к существенным недостаткам действующей системы отчетности в органах внутренних дел.

Вместе с тем хотелось бы обратить особое внимание на то, что существенное отличие размера причиненного ущерба в 2006 году (по оконченным расследованием уголовным делам) по сравнению с 2005 годом (на момент возбуждения уголовных дел) говорит не о снижении эффективности работы органов внутренних дел, поскольку количество выявленных преступлений в целом увеличилось, а свидетельствует о повышении качества расследования и оперативного сопровождения возбужденных уголовных дел в части значительного возмещения причиненного ущерба еще на стадии предварительного следствия, так как на момент возбуждения уголовных дел (данные ГИАЦ МВД России по итогам 2005 года) размер причиненного ущерба значительно выше, чем по оконченным расследованием уголовным делам (данные ГИАЦ МВД России по итогам 2006 года).

Кроме того, действующая с 01.01.2006 года система учета размера причиненного материального ущерба по оконченным расследованием уголовным делам, без указания размера ущерба на момент возбуждения уголовных дел, не позволяет объективно оценить значимость выявленных преступлений.

Таким образом, в целях упорядочения статистических учетов оперативно-розыскной деятельности подразделений органов внутренних дел представляется целесообразным:

1. В форме 1А статистики ГИАЦ МВД России исчислять размер причиненного материального ущерба как на момент возбуждения уголовных дел, так и по оконченным расследованием уголовным делам.

2. В форме 1А статистики ГИАЦ МВД России, в соответствии с классификатором отраслей, предусмотреть учет количества выявленных преступлений и размера ущерба как на момент возбуждения уголовного дела, так и по оконченным расследованием уголовным делам по каждой отрасли в отдельности.

3. Добавить в классификатор отраслей все подотрасли сферы ТЭК:

- нефтедобыча, переработка и реализация нефтепродуктов;
- химическая и нефтехимическая промышленность;
- добыча, переработка, транспортировка и реализация газа;
- недропользование;
- электроэнергетика;
- горнодобывающая и угольная промышленность.

4. Установить ежеквартальную периодичность обновления статистической отчетности с учетом вышеперечисленных изменений.

Внесение указанных изменений позволит объективно оценивать результаты оперативно-розыскной деятельности органов внутренних дел в целом, а также в сфере ТЭК.