ИСПОЛЬЗОВАНИЕ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕДУПРЕЖДЕНИИ ПРЕСТУПНОСТИ

В. СТЕРПУ,
докторант, Государственный университет Молдовы

SUMMARY

This article addresses the problem of development in the field of informational technologies and ensure it's safety as a priority element of the national policy of many countries. However, high technology and global computer networks have created conditions for criminals who invented new ways to commit and conceal the crimes not only at national but also at the international level. Committing offences in this area criminals apply techniques and tools linked to computer equipments and information lines of communication, including computer networks. Crime in the informational technology sphere today cause significant material and moral harm to the individual, society.

* * *

В данной статье рассматривается проблема развития информационной сферы и обеспечения ее безопасности как приоритетный фактор национальной политики многих стран. Вместе с тем высокие информационные технологии и глобальные компьютерные сети создали условия для преступников, которые изобрели новые способы совершения и сокрытия преступлений не только на национальном, но и на международном уровне. Для совершения преступлений в этой области преступниками применяются технические приемы и средства компьютерной техники и используются информационные линии связи, в том числе компьютерные сети. Преступления в информационной сфере сегодня наносят значительный материальный и моральный вред личности, обществу, государству.

Современное информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, экономическими и финансовыми структурами, органами государственной власти. Развитие информационной сферы, обеспечение ее безопасности стало одним из приоритетов национальной политики многих стран. Вместе с тем высокие информационные технологии и глобальные компьютерные сети создали условия для преступников, которые изобрели новые способы совершения и сокрытия преступлений не только на национальном, но и на международном уровне. Для совершения преступлений в этой области преступниками применяются технические приемы и средства компьютерной техники и используются информационные линии связи, в том числе компьютерные сети. Преступления в информационной сфере сегодня наносят значительный материальный и моральный вред личности, обществу, государству[1].

Совершенствование средств вычислительной техники представляет собой основу новой информационной технологии, которая применяется для создания комплексных автоматизированных систем информационного обеспечения, сводящих участие человека в этом процессе к минимуму (компьютер в автоматизированном режиме собирает, передает, обрабатывает, хранит и по запросу выдает необходимую информацию). Ныне компьютеры становятся основным инструментом для управления информацией и ее обработки, а человечество вплотную приблизилось к новому этапу своего развития - этапу безбумажной информатики.

Сегодня организованные преступные группы способны использовать возможности быстро развивающихся технологий в противоправных целях. Киберпреступность приобрела трансграничный характер, а главные проблемы предупреждения этого явления - нехватка знаний о масштабах проблемы и различия в национальных системах.

Киберпреступность можно

охарактеризовать как один из серьезнейших вызовов правоохранительной системе. И в этих условиях возрастает необходимость разработать соответствующую международную конвенцию. Из цитируемых источников выявляется, что государствам необходимо развивать свой потенциал, и в этом деле им могло бы помочь ЮНОДК (United Nations Office on Drugs and Crime) путем оказания технической экспертной помощи и оперативной поддержки. Одним из эффективных способов наращивания всеобъемлющего и устойчивого потенциала государств в целях пресечения киберпреступности мог бы стать глобальный план действий по наращиванию потенциала с участием ключевых учреждений и партнеров.

Следует признать, что быстрое развитие технологий имеет многие бесспорные преимущества. В то же время такое развитие позволило новыми способами совершать традиционные виды преступлений, включая мошенничество и распространение материалов, содержащих детскую порнографию, а также породило новые виды преступлений, таких, как хакерство, спаминг, “фишинг” (использование в мошеннических целях поддельных сайтов или рассылки сообщений со ссылками на такие сайты), цифровое пиратство, злонамеренное распространение вирусов и другие атаки на критически важную информационную инфраструктуру.

В докладе о работе двенадцатого Конгресса ООН по предупреждению и уголовному правосудию отмечалось, что террористические организации и организованные преступные группы поставили быстрое научно-техническое развитие на службу своей преступной деятельности. Итак, киберпреступность представляет угрозу для экономики и жизненно важной инфраструктуры, а также подрывает доверие к институциональным структурам и социально-культурному благополучию.

Все чаще говорится о возможности применения информационных технологий в правоохранительной области, в частности речь идет о системах электронного слежения и наблюдения, искусственном интеллекте и электронных средствах выявления подозрительных финансовых операций и установления IP-адресов. Вместе с тем для расследования киберпреступлений и привлечения к ответственности за их совершение необходимы новые навыки и процессуальные механизмы, в частности наличие возможности для сбора и анализа цифровых доказательств и их использования в производстве по уголовным делам. Надо подчеркнуть и важность защиты частной жизни и прав человека в рамках борьбы с киберпреступностью. Конечно, достижение такого результата возможно только в тесном международном сотрудничестве, а именно при принятии государствами мер по повышению эффективности оказания взаимной правовой помощи и сотрудничества в правоохранительной области.

Наиболее уязвимыми для киберпреступности являются развивающиеся страны. В цитируемом документе подчеркивается, что развитым странам следует в срочном порядке активизировать деятельность по оказанию помощи в наращивании потенциала, особенно в отношении подготовки сотрудников правоохранительных органов, прокуроров и судей. Частный сектор, в том числе поставщики услуг, должны с полной ответственностью участвовать в этой работе. Имеется ряд механизмов, как виртуальный форум для стран Азии, созданный при помощи ЮНОДК, учебный веб-модуль Международной ассоциации прокуроров и подготовленная Международным союзом электросвязи подборка материалов по законодательству в области борьбы с киберпреступностью[2].

Успешность любого вида правоохранительной деятельности во многом зависит от степени обеспечения ее соответствующей длительно накопленной и систематизированной информацией о преступлениях, совершенных в прошлом, причастных к ним лицах, средствах и способах их совершения, различных следах преступлений и объектах, связанных с криминальными событиями, а также от возможности и умения следователя пользоваться подобной информацией в своей деятельности для выявления, розыска и

отождествления интересующих их явлений и объектов.

Указанная информация обычно содержится в специфических картотеках (следотеках), списках, коллекциях, в памяти ЭВМ и иных собирательных системах. Такого рода специфические системы справочных, розыскных и иных криминалистически значимых данных для раскрытия, расследования и предупреждения преступлений, являющихся своеобразными «хранилищами» подобной информации, получили в криминалистике название криминалистически значимых учетов. Научно разработанная система учетов сформировала целую регистрационную систему, называемую криминалистической регистрацией. Она представляет собой научно разработанную систему справочных, розыскных и иных криминалистических учетов объектов-носителей криминалистически значимой информации, используемой для раскрытия, расследования и предупреждения преступлений[3].

Предупреждение преступлений является одним из наиболее эффективных путей борьбы с преступностью и представляет собой весьма сложный и многоплановый комплекс мер различного характера. Одной из основных частей этого комплекса является криминалистическое предупреждение преступлений. Криминалистическое предупреждение – это система «научных положений и практических рекомендаций о закономерностях разработки и использования в уголовном судопроизводстве технических средств, тактических и методических приемов для предотвращения подготавливаемых преступлений», а также «своевременного обнаружения, полного раскрытия и качественного расследования совершенных преступлений, выявления и устранения в процессе расследования обстоятельств, способствующих совершению и раскрытию преступлений»[4].

Отметим, что в последнее время большинство ученых сошлись во мнении, что понятия «предупреждение преступлений» и «профилактика преступлений» имеют очень близкое содержание, поэтому используют данные понятия как синонимы. В другом важном вопросе, касающемся соотношения криминалистического и криминологического предупреждения, в науки нет единства точек зрения. По мнению Махтаева М.Ш. не существует четкой границы между криминологическим и криминалистическим предупреждением преступлений, подобно тому, как не существует жесткого разграничения между криминалистикой и уголовным процессом[5]. Об отсутствии такого разграничения «в силу взаимного влияния и проникновения» писал также Белкин Р.С. [6]. Ранее аналогичную позицию отстаивал Зудин В.Ф., писавший, что «четкой границы в сфере криминологической и криминалистической профилактики нет»[7]. В то же время Иванов И.И. выступает против подобного расширения рамок криминалистической профилактики. По сути, это отражает различные взгляды на предмет криминалистического предупреждения преступлений. Можно выделить положения, объединяющие различные точки зрения и заключающиеся в том, что теоретической и прикладной проблематикой криминалистического предупреждения преступлений является разработка средств, методов и приемов, использование которых способно обеспечить эффективное осуществление комплекса предупредительных мероприятий. Проблематика криминалистического предупреждения преступлений имеет пограничный характер, получаемые результаты представляют ценность как непосредственно для криминалистики, так и для уголовного процесса и теории оперативно-разыскной деятельности. Как следствие, разрабатываемые приемы и методы применяются, во-первых, следователями и органами дознания; во-вторых, оперативными работниками; в-третьих, специалистами и экспертами; в-четвертых, сотрудниками прокуратуры; в-пятых, сотрудниками суда.

В области предупреждения преступлений, к примеру в Российской Федерации, используются автоматизированные информационные дактилоскопические системы (АДИС) на основе персональных компьютеров, с помощью которых можно автоматически кодировать отпечатки и следы пальцев рук, сохранять их изображение в памяти и про-

изводить качественный сравнительный анализ. Наиболее известными являются «Папилон», разработчик - ТОО «Системы Папилон» и «Сонда-Фрес», разработчик - СП «Совиндейта».

Внедрение в практику органов внутренних дел компьютерных систем составления субъективных портретов позволяет получить ряд преимуществ по сравнению с традиционными системами. Использование субъективных портретов существенно расширяет возможности при установлении личности преступников, скрывшихся с мест происшествия, и иных лиц, имеющих отношение к расследуемому событию. Субъективный портрет является специфическим объектом, используемым при отождествлении личности по признакам внешности[8].

Первой в Российской Федерации из компьютерных систем построения композиционных портретов стала система «ЭЛЛИ» (элементы лица). В дальнейшем появились «ФОТОРОБОТ» (разработчик МГУ им. Э. Баумана, Москва) и «КРИС» (совместная разработка УВД Юго-Западного административного округа Москвы и УВД Рязанской области).

В 1995 году в Московском Государственном Университете им. Баумана была разработана новая версия (2.0) компьютерной системы «Фоторобот-С» (сокращенно «ФРС-2»). Результаты тестирования показали, что система «ФРС-2» успешно объединяет в себе различные базы данных: базу полутоновых изображений и базу рисованных элементов внешности. Новая компьютерная система «ФРС-2» позволяет составлять субъективные портреты, максимально приближенные по своим изобразительным свойствам к фотографии[9].

Типовые элементы внешности - полутоновые или многоградационные изображения, представляют собой «маски-картинки». С одной стороны, смонтированный в английской системе «E-FIT» субъективный портрет не воспринимается как фотографическое изображение реального человека; с другой стороны, «объемность» портрета способствует его восприятию определенной категорией очевидцев[10].

С появлением компьютеров в подразделениях внутренних дел России была внедрена программа «CLIENT», позволяющая осуществлять пополнение центральной базы и исполнение запросов к центральной базе данных с рабочих мест.

Создание единого информационного пространства позволяет получать интегрированные данные на любой объект, учтенный в информационной базе данных, качественно меняет уровень работы всех подразделений. Внедренная база данных «FLINT» является распределенной базой данных, содержащей информацию, необходимую для оперативно-розыскной и аналитической деятельности.

Все же самой модернизированной и успешной технологией в предупреждении и борьбе с преступностью обладает международная организация Интерпол. В 2007 году она достигла всеобщего подключения к 1-24/7 глобальной полицейской системе коммуникации. Уже тогда Интерпол насчитывал 186 членов. Его главная цель – расширение допуска к этой системы заинтересованных сотрудников всей планеты.

Используя внедренные технические задачи, так называемые MIND и FIND- мобильные и стационарные базы данных Интерпола, эти сотрудники могут сейчас иметь допуск к базам данных сворованных и потерянных документов, сворованных автомобилей и данные о лицах, находящихся в розыске. К концу 2007 года система MIND/FIND полностью действовала в 20 государствах. Например, Швейцария выявила 1700 поддельных паспортов из 45 государств на 6 континентах[11].

Также в предупреждении преступности очень эффективно действует обращение внимания граждан на существующие и совершенные преступления через СМИ и Интернет. Довольно хорошо известна успешная практика сообщения о совершении преступления через Интернет в ряде стран членов Европейского Союза и США. Данные могут быть отправлены в нужное подразделение внутренних дел, при этом сохраняя свою анонимность. Например, на официальном сайте ФБР США подробно объяснены схемы потенциальных преступлений, знание о которых может предохранить

граждан от моральных и материальных ущербах. Интерактивные игры и опросы на сайте ФБР позволяют гражданам с разным уровнем подготовки понять схемы потенциальных преступников, предохранять себя, близких и свое имущество.

В многогранном комплексе мер по совершенствованию деятельности органов внутренних дел все большее значение приобретает широчайшее применение компьютеров. Компьютер помогает человеку логически и более глубже мыслить; не заменяя его, делает наиболее оптимальными и более действенными деяния человека. С появлением компьютеров и компьютерных сетей существенно возросла скорость обработки и передачи информации. Таким образом, отделы внутренних дел и используемая им техника должны рассматриваться во взаимосвязи и взаимодействии, а это позволит наиболее эффективно и качественно работать с разными информационными источниками.

Литература:

1. Стратегия развития информационного общества в Российской Федерации. Утверждена Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 // Российская газета, 16 февраля 2008.

2. Доклад о работе двенадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию. Сальвадор, Бразилия, 12-19 апреля 2010 года, п.155. (http://www.unodc.org/documents/crime-congress/12th-Crime- Congress/Documents/A_CONF.213_18/V1053830r.pdf, цитировано 20 декабря 2011).

3. Андрюшин Х.А., Информатика и математика для юристов. Москва, 2002.С.245.

4. Иванов И.И. Криминалистическая превенция (генезис, теоретические и методологические основы, перспективы развития в сфере нового уголовно-процессуального законодательства) СПб., 2003.С.234.

5. Махтаев М.Ш. Основы теории криминалистического предупреждения преступлений. Москва, 2001. С.356.

6. Белкин Р.С. Курс криминалистики. Москва, 1997. С.237.

7. Зудин В.Ф. Социальная профилактика преступлений: Криминологические и криминалистические проблемы ; под ред. В.И. Федулова. Саратов, 1983.С.324.

8. Снетков В.А. «ИКР-2» в практике раскрытия преступлений. Москва, 1991.С.374.

9. Орлов Н.Н. Практика использования программы «ФРС» для составления компьютерных субъективных портретов разыскиваемых лиц. Москва, 1995.С.134.

10. Кочетыгов А.В. Влияние графической доработки компьютерного субъективного портрета. Москва, 1995. С.256.

11. Interpol. Annual report, 2007, p.8. www.interpol.int (цитировано 10 декабря 2011).