Типичными подготовительными действиями (они же могут служить и при учете тех либо иных признаков следовой картины), совершаемыми при нарушении границы с применением указанной группы способов, являются:

предварительное изучение режима охраны государственной границы, порядка несения службы контролерским составом, отдельными часовыми и иными военнослужащими органов пограничной службы;

неоднократное вызывание ложного срабатывания охранной сигнализации с целью усыпления бдительности пограничного наряда;

использование естественного повреждения или разрушения основного ограждения и прилегающей к нему территории вследствие таяния снега или обильных дождей (образовавшихся ям, промоин и т. п.);

использование благоприятных погодных условий (снегопада, метели, тумана), плохой видимости, заранее подготовленных в качестве маскировочных средств простыней, халатов, накидок и т. п.;

приискание, изготовление и использование различных предметов и приспособлений, с помощью которых можно преодолеть линию охраны государственной границы (длинных досок, трапов, крюков, лестниц, веревок, шестов и т. п.).

Почти каждое четвертое незаконное пересечение государственной границы совершается на тех участках пропуска, где имеет место постоянное движение автомашин, железнодорожных составов и других транспортных средств. Для совершения незаконного пересечения границы нарушители укрываются самостоятельно (либо с помощью других лиц) под капотом транспортного средства, в пустых топливных баках, в кабине (под сидением), под различными грузами, в древесной таре, в цистернах, бочках, специально изготавливаемых тайниках и т. п. Время на подготовку таких незаконных пересечений границы составляет от трех дней до двух недель. Большинство нарушений границы совершается в группе из двух-трех человек.

Пересечение границы осуществляется в наиболее удобное для этого время, как правило ночью, в сильный дождь, снегопад, туман и т. п.

Незаконное пересечение государственной границы имеет свои пространственно-временные характеристики.

Криминалистическое значение места совершения незаконного пересечения границы состоит в том, что на нем обнаруживаются приобретающие в последующем доказательственное значение следы и иные объекты. Полученная на месте преступления информация позволяет устанавливать его механизм, обстоятельства, способ и время совершения. Кроме этого, она способствует выявлению характера действий и личностных свойств преступника. Место совершения незаконного пересечения границы в криминалистической характеристике рассматриваемого вида преступления может отражаться различными, в том числе детализирующими, признаками.

Исходя из задач расследования преступлений, в криминалистической характеристике незаконного пересечения границы целесообразно учитывать сведения о месте его подготовки, совершения и сокрытия, а также местах уклонения преступников от уголовной ответственности и наказания за содеянное. При этом важными являются сведения и о маршрутах передвижения преступников и субъектов сокрытия преступлений.

На современном этапе разработки данной проблемы важно учитывать, что рассмотрение в криминалистической характеристике незаконного пересечения границы сведений о закономерностях соотношения и связях между местами их совершения, прежнего места жительства преступника, мест сокрытия и уклонения от уголовной ответственности и наказания и т. д. создает хорошие предпосылки для более полного и глубокого познания механизма совершенного преступления и особенностях его проявления.

Время совершения преступления имеет уголовно-правовое, уголовно-процессуальное и криминалистическое значение.

В уголовном праве время рассматривается в узком аспекте – время совершения преступления. Оно определяется как очерченный определенными рамками промежуток времени, в котором имели место преступные деяния. Его криминалистическое значение определяется тем, что в совершении незаконного пересечения границы наблюдается определенная избирательность во времени действий преступников (в определенное время объект меньше охраняется, отключена сигнализация и т. д.).

Данные о времени совершения и сокрытии преступлений позволяют верно оценивать обстоятельства события незаконного пересечения границы, сузить круг соучастников, субъектов сокрытия преступления и т. д.

Интенсивность незаконных нарушений границы возрастает, как правило, в весенне-летний период. В это время условия облегчают нарушителям совершение незаконного пересечения границы и позволяют длительное время скрываться от преследования.

Почти каждое третье преступление совершается в субботние, воскресные и праздничные дни, и около половины – ночью. Используется именно то время, когда надзор за государственной границей является ослабленным.

При подготовке к незаконному пересечению границы устанавливаются лица, допускающие отклонения от уставных требований несения пограничной службы, не выполняющие режимных требований, предпринимаются попытки вступления с ними в нелегальные связи и т. д. Необходимо учитывать, что в таких случаях действия этих субъектов ограничиваются не только подготовкой либо совершением преступления, но и играют существенную роль в его сокрытии, а также в уклонении от уголовной ответственности лиц, совершивших его.

Как правило, лицом, намеревающимся совершить нарушение границы, продумываются различные варианты и способы преодоления препятствий, определяются обстоятельства (условия), которые можно использовать при осуществлении преступного замысла, прогнозируются дальнейшие действия в случае его успешного совершения, а также действия по сокрытию преступления.

УДК 351.746

В.Б. Шабанов

ЕДИНОЕ ГЛОБАЛЬНОЕ ИНФОРМАЦИОННОЕ КРИМИНАЛИСТИЧЕСКОЕ ПРОСТРАНСТВО КАК СТРАТЕГИЧЕСКОЕ ПОЛЕ КРИМИНАЛИСТИЧЕСКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Глобальные информационные системы связывают мир в единое целое и делают все государства информационно взаимозависимыми, заставляя проявлять максимум внимания к качеству информационного взаимодействия в различных сферах жизнедеятельности общества.

В эпоху всеобщей информатизации и построения информационного общества единая информационная среда (пространство) является одним из важнейших государствообразующих признаков, обязательным условием и характеристикой самого информационного общества.

Единое информационное пространство (ЕИП) является:

важным обязательным признаком и предпосылкой успешного формирования информационного общества, необходимым условием вхождения в мировое информационное сообщество;

главным условием сохранения информационного суверенитета страны и укрепления государственности;

стратегическим полем информационно-криминалистических технологий.

Группа наиболее развитых стран (США, Канада, Япония, Германия, Франция, Англия, Италия), считая создание единого информационного пространства одной из приоритетных задач XXI в., договорились о сотрудничестве в создании глобальной информационной инфраструктуры на базе следующих основополагающих принципов:

поддержка динамичной конкуренции;

стимулирование частных инвестиций;

обеспечение открытого доступа к сетям и универсального доступа к услугам;

равенство возможностей для всех граждан;

признание и учет различий, включая культурное и лингвистическое разнообразие;

признание необходимости международного сотрудничества, особенно с менее развитым странам.

Политика информационной безопасности зависит от системы угроз. Информационная безопасность должна стать приоритетной задачей государства, за решение которой несет ответственность весь государственный аппарат. При этом должна быть определена та информация, которая нуждается в защите, и уточнено, какие меры, технологические либо процедурные, могут решить эту задачу. Например, следует организовать регистрацию инцидентов и предвидеть реакцию служащих, ответственных за обеспечение информационной безопасности. Необходимо интерпретировать и прогнозировать то, что ожидается с точки зрения поставленной цели.

Государственная информационная политика – это часть внутренней и внешней политики государства, которая состоит в регулировании информационных потоков и информационной деятельности различных государственных, общественных, частных структур и организаций информационного профиля. Однако значительный конструктивный потенциал информационной политики еще не нашел адекватной оценки и необходимого уровня практической реализации. Ключевой проблемой в данной области является разработка концепций государственной информационной политики и системы мероприятий по ее активации.

Главные направления и способы государственной информационной политики:

обеспечение доступа граждан к информации;

укрепление материально-технических, финансовых, организационных, правовых и научных основ информационной деятельности;

обеспечение эффективного использования информации;

криминалистическое и правовое обеспечение информационной безопасности;

содействие постоянному обновлению, обогащению и хранению национальных информационных ресурсов;

создание общей системы охраны информации;

содействие международному сотрудничеству в области информации.

Государственную информационную политику разрабатывают и осуществляют органы государственной власти общей и специальной компетенции.

Система угроз должна системно нейтрализоваться, изучаться, прогнозироваться, моделироваться, профилактироваться комплексом криминалистических и иных мероприятий, отслеживаться оперативно-розыскными службами.

Правовая охрана и защита прав и интересов субъектов при формировании и сохранении единого информационного пространства страны должна осуществляться в привязке к основным объектам защиты в области информационной безопасности: защите информации, защите от информации, защите информационных систем. Рассмотрим лишь особенности организации и осуществления защиты единого информационного пространства страны в целом, а также прав и интересов государства по его формированию и сохранению, т. е. случай, когда единое информационное пространство страны выступает одним самостоятельным объектом защиты.

С учетом изложенного попытаемся суммировать общие проблемы формирования и сохранения единого информационного пространства страны, требующие нормативно-правового регулирования и его защиты как единого целого (по В.Н. Лопатину).

Нормативные акты, регулирующие формирование и сохранение единого информационного пространства страны и его защиту в целом и по отдельным объектам, противоречивы и неполны. Необходимы единый понятийный словарь, единые концептуальные подходы в определении содержания объектного состава и структуры единого информационного пространства и его сопряжения на всех уровнях.

Необходимо определить основу, ось и приоритеты разноуровневой интеграции единого информационного пространства. Если в качестве основы такого построения использовать информационные системы (в узком смысле это слова), то возможна такая ось: мировое ЕИП (интернет) – ЕИП СНГ (автоматизированная система информационного обмена между государствами – участниками СНГ (АСИО СНГ)) – ЕИП Союзного государства (ИТКС, ИКС, ГИС) – региональное ЕИП (автоматизированная информационная система региона (АИС региона)) – муниципальное ЕИП (АИС города, района). Здесь наряду с едиными протоколами и оборудованием нужны единые правовые принципы и правила функционирования и взаимодействия.

Необходимо нормативно-правовое закрепление ответственности за формирование ЕИП на каждом уровне за руководителями ведомств и администрацией регионов, а также назначение государственных заказчиков по важнейшим направлениям развития единого информационного пространства России и Беларуси и разработка ими проектов программ.

Для координации этой работы назрела необходимость формирования авторитетного (как по составу, так и по полномочиям) общенационального центра координации формирования и сохранения ЕИП страны (первым об этом заявила профессор И.Л. Бачило, доктор юридических наук ИГП РАН).

Необходимо также создать межотраслевые, межрегиональные и региональные советы по формированию и использованию государственных информационных ресурсов.

Необходима организация полноценного мониторинга состояния информационного пространства страны на всех уровнях и по всему объектному составу (в том числе организация государственной статистической отчетности по информационным ресурсам, по информатизации, производству информационных продуктов и услуг, состоянию информационной индустрии), информирование общества по результатам мониторинга. Это позволит организовать широкое обсуждение проблем формирования и развития единого информационного пространства с привлечением средств массовой информации, проведение конкурсов на лучшие предложения,

Нужна разработка комплекса информационных стандартов (в том числе в области информационной безопасности); развитие системы сертификации информационных продуктов, систем и услуг; создание системы лицензирования деятельности организаций по отдельным направлениям формирования ЕИП и его защиты в соответствии с законодательством; экспертиза проектов государственных информационных систем и ресурсов.

Необходимо ограничить информационную экспансию крупных зарубежных фирм, их стремление навязать национальным информационным и телекоммуникационным системам собственные условия функционирования в мировом информационном пространстве.

В зависимости от угроз можно рассматривать следующие виды безопасности человеческого общества: ядерную, экологическую, политическую, технологическую, экономическую, криминалистическую и др. Их залогом является криминалистическое обеспечение информационной безопасности.

УДК 343.983

Т.Н. Шамонова

ИЗУЧЕНИЕ СПЕЦИФИКИ СЛЕДОВОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ НАСИЛЬСТВЕННОГО ХАРАКТЕРА

Ознакомление с методиками расследования преступлений, связанных с насилием (учет и насильственно-корыстных, и насильственных сексуальных деяний), показало, что в учебниках криминалистики недостаточно внимания уделяется следам и использованию их в доказывании. В криминалистической характеристике данных преступлений в большинстве случаев указаны следующие элементы: способ совершения и