



Душин
Иван Владимирович,
оперуполномоченный Управления «К»
БСТМ МВД России, капитан полиции

Деятельность Управления «К» в области профилактики и борьбы с преступлениями в сфере информационных технологий

В настоящее время проблеме киберпреступности уделяется все больше внимания, что неудивительно с учётом роста ее во всём мире. Появляются новые виды компьютерных преступлений, наблюдается стремительное проникновение информационных технологий в общеуголовную преступность. Операторы связи, наращивая темпы внедрения телекоммуникационной техники и информационных услуг, невольно вооружают преступников новыми возможностями. Криминалитет умело использует эти возможности для многократного усиления динамики и сокрытия своей деятельности.

Сегодня проблема защиты граждан, их прав и свобод от преступных посягательств с использованием новых информационных технологий стоит как никогда остро. Информационное пространство не имеет границ, и поэтому ни одно государство самостоятельно не может решить проблемы обеспечения его безопасности. МВД России неоднократно выступало с предложениями, направленными на развитие и совершенствование информационного обмена в области противодействия преступлениям в сфере информационных технологий.

Российские инициативы в том или ином виде фигурируют и реализуются в форматах таких международных организаций, как ООН, «Группа восьми», ЕС, ОБСЕ, Совет Европы, АТЭС, ШОС, ОДКБ, СНГ. Речь идет об организации расследований киберпреступлений с обязательным направлением оперативной информации в страну местонахождения правонарушителя в целях возбуждения уголовного дела и скорейшего осуждения преступников, а также о противодействии анонимности пользователей в информационно-телекоммуникацион-

ном пространстве. При обсуждении данных проблем МВД России выступает с позиции строгого соблюдения принципов неприменения силы, невмешательства во внутренние дела государств, исключения двойных стандартов в оценках преступных деяний, уважения прав и свобод человека, недопущения использования ИТ-технологий в целях, противоречащих Уставу ООН.

В настоящий момент происходят изменения в российской законодательной базе, регулирующей данную область. Наиболее заметные изменения внесены в Уголовный кодекс (Федеральный закон «Об информации, информационных технологиях и о защите информации»). С целью ограждения детей от информации, способной причинить вред их здоровью и развитию, вступил в силу Федеральный закон от 28 июля 2012 г. №139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации». Принятые новеллы ещё на этапе их подготовки вызвали волну недовольств в Интернет-СМИ и со стороны крупных российских ИТ-компаний. Согласно принятому закону, в ряд нормативных актов вносятся положения, главной идеей которых является создание единого реестра запрещённых Интернет-ресурсов и блокирование доступа к ним. В реестр вносятся ссылки на страницы или доменные имена, содержащие материалы с порнографическими изображениями несовершеннолетних, пропагандой употребления и изготовления наркотиков, способами и призывами к совершению самоубийства.

Параллельно с процессом нововведений в законодательные осно-

вы регулирования информационного пространства эволюционирует и преступность. Официальная статистика показывает, что за первое полугодие 2012 года, по сравнению с аналогичным периодом прошлого года, по отдельным видам преступлений, совершенным в сфере телекоммуникаций и компьютерной информации, складывается следующая картина: количество преступлений, связанных с созданием, использованием и распространением вредоносных программ (ст. 273 УК РФ), увеличилось на 46,9%; с оборотом материалов с порнографическими изображениями несовершеннолетних (ст. 242.1 УК РФ) — на 6%. В то же время снизилось количество преступлений, связанных с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), а также нарушением авторских и смежных прав (ст. 146 УК РФ) на 11,3% и 32,8% соответственно. Совершенно очевидно, что долгосрочные прогнозы развития криминогенной ситуации в сфере телекоммуникаций и компьютерной информации в России будут в полной мере совпадать с общемировыми. Основа для такой уверенности — однотипные процессы внедрения информационных технологий во всех странах — компьютеры, протоколы, сервисы должны быть и являться одинаковыми, иначе они не будут взаимодействовать, не будет глобальной сети.

Для противодействия преступлениям в сфере информационных технологий в структуре МВД России уже более 14 лет функционирует специальное подразделение — Управление «К». Основными направлениями деятельности Управления являются: борьба с преступлениями в сфере компьютерной информации: всевозможными мошенничествами с использованием сети Интер-



нет, хакерскими атаками, распространением вредоносных программ; борьба с распространением в сети Интернет порнографических материалов с участием несовершеннолетних; пресечение противоправных действий в информационно-телекоммуникационных сетях, например участвовавшие телефонные мошенничества; борьба с незаконным оборотом радиоэлектронных средств и специальных технических средств для негласного получения информации; борьба с нарушениями авторских и смежных прав в информационной сфере (яркий пример — пиратская продукция: оптические диски и нелегальное программное обеспечение); борьба с международными преступлениями в ИТ-сфере.

Говоря про деятельность Управления «К», необходимо отметить, что подразделение занимается не только борьбой с уже совершенными преступлениями, но и уделяет большое внимание профилактике противоправных деяний и защите граждан от мошенничества в ИТ-сфере. В феврале 2012 года по инициативе Управления «К» запущена Всероссийская комплексная кампания «Безопасный Интернет». В рамках этой кампании был выпущен ряд брошюр, в которых специалистами даются рекомендации по защите компьютера от вредоносных программ, а также противодействию телефонному и компьютерному мошенничеству.

В настоящее время Интернет для большинства граждан стал незаменимым и основным источником информации. К сожалению, свободный доступ к любой информации приводит к тому, что пользователь может легко стать жертвой мошенников. Чаще всего опасности подвергаются дети по своей наивности и незнанию простейших правил безопасности в виртуальном пространстве. В связи с этим повышенного внимания требует проблема бесконтрольного доступа детей и подростков к информационным и развлекательным сетевым ресурсам, среди которых могут скрываться мошеннические, вредоносные или порнографические сайты. В рамках комплексной кампании запущена школьная образовательная программа «Уроки безопасного Интернета», в ходе которой сотрудники Управления в доступной игровой форме объясняют ученикам 3 и 4 классов правила безопасности использования

Интернета и те угрозы, с которыми они могут столкнуться в социальных сетях, на форумах и сайтах. Сотрудниками Управления «К» разработаны специальные учебные пособия и программное обеспечение, которые рекомендованы для изучения в российских школах.

Кроме того Управлением «К» в регионах проводится серия круглых столов по теме «Интернет: технология безопасности» с участием представителей территориальных подразделений ОВД, общественных советов при территориальных подразделениях МВД России, региональных органов исполнительной власти, общественных организаций и представителей Интернет-сообщества. Основными проблемами, обсуждаемыми на этих встречах, являются: борьба с детской порнографией в сети, использование информационных технологий для защиты от киберпреступлений, решение вопросов интеллектуальной собственности и авторских прав в сети и т.п.

Говоря о борьбе с детской порнографией и педофилией в сети Интернет, следует отметить, что это одно из наиболее актуальных направлений деятельности Управления «К» МВД России, поскольку данный вид преступлений носит особо характерный и социально опасный характер. Распространение детской порнографии — это преступление, поставленное вне закона во всем мире. В 2012 году сотрудниками Управления «К» МВД России проводится Всероссийская операция «Сорняк», направленная на пресечение распространения детской порнографии в Интернете посредством пиринговых сетей. Только за 9 месяцев 2012 года выявлено 148 пользователей из 53 регионов России. Подготовлено для возбуждения 180 материалов уголовных дел, в большинстве регионов проведены оперативно-розыскные мероприятия и следственные действия по пресечению деятельности и задержанию лиц, совершающих указанные преступления. По материалам, направленным в следственные органы, возбуждено 96 уголовных дел в отношении педофилов. В ходе работы зафиксировано около 1200 иностранных пользователей из 62 государств. Основная доля пользователей приходится на европейские страны, США и Канаду. По каналам Национального контактного пункта Управления «К» в адрес правоохранительных органов этих стран на-

правлены материалы о фактах преступной деятельности их граждан. Коллеги проинформированы о заинтересованности Управления «К» в проведении совместных расследований.

В продолжение темы международного сотрудничества 1 июня 2012 года состоялась встреча представителей Управления «К» при участии Уполномоченного при Президенте России по правам ребёнка П. А. Астахова с представителями по правоохранительным вопросам посольств иностранных государств и офицеров связи из 27 стран мира. В ходе мероприятия российской стороной предложены конкретные пути и направления взаимодействия, включающие в себя обмен опытом расследования информационных преступлений и профессиональную подготовку сотрудников правоохранительных органов.

Актуальность вопросов обеспечения информационной безопасности не снижается, а только возрастает. Масштаб разрушительных последствий от использования возможностей информационно-коммуникационных технологий в криминальных, враждебных или террористических целях трудно переоценить. Поэтому вопрос создания адекватных механизмов регулирования этого огромного виртуального пространства, налаживания горизонтального взаимодействия между представителями профессионального сообщества, научного сектора и государственных структур является на сегодняшний день задачей, от решения которой зависит не только уровень ИТ-преступности, но и в целом степень защищённости российского государства.