Мурашбеков О. Б.,
докторант Института послевузовского образования, капитан полиции
(Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова)

ПРОБЛЕМЫ БОРЬБЫ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ

Правоохранительным органам становится известно о деяниях в области киберпреступности из сообщений частных лиц или организаций, ставших жертвами такой деятельности. Полиция получает сообщения о виктимизации в результате киберпреступности в одном или более процентах случаев. Исследования показывают, что 80 % частных лиц, ставших жертвами киберпреступности, в полицию о преступлении не сообщают. Это объясняется тем, что они не знают о виктимизации и о механизмах сообщения информации, ощущают стыд или неловкость в связи с тем, что стали жертвами преступников, а корпорации опасаются возможного репутационного риска.

Государственные органы многих стран мира сообщают об инициативах, направленных на повышение уровня представления информации о совершении преступлений, в том числе о системах, позволяющих сообщать о преступлениях по Интернету и «горячим» телефонным линиям, кампаниях по повышению информированности общественности, контактах с частным сектором и активизации информационно-пропагандистской деятельности полиции и обмене информацией. Однако меры борьбы с киберпреступностью, принимаемые в порядке реагирования на совершенные преступления, должны сопровождаться среднесрочными и долгосрочными тактическими расследованиями в отношении рынков преступности и разработчиков преступных схем. Правоохранительные органы развитых стран работают в этой области, в том числе используя действующие под прикрытием подразделения по выявлению правонарушителей на сайтах социальных сетей, в чатах и при обмене мгновенными сообщениями и материалами совместного пользования («P2P»)[i]. Трудности при расследовании киберпреступлений связаны с использованием преступниками новаторских преступных методов, сложностями в получении доступа к электронным доказательствам и с внутренними ограничениями в отношении ресурсов, потенциала и материально-технических возможностей. Подозреваемые часто используют технологии анонимизации и запутывания следов, и новые технологии быстро получают распространение в преступном мире благодаря онлайновым преступным рынкам.

Для расследования киберпреступлений правоохранительным органам необходимо использовать как традиционные, так и новые методы работы полиции. В то время как некоторые следственные действия могут быть осуществлены на основании традиционных полномочий, многие процессуальные положения, в основе которых лежит пространственный, ориентированный на предметы подход, трудно применять в ситуациях, связанных с хранением электронных данных и потоками данных в режиме реального времени. Существует несколько методов расследования киберпреступлений, начиная с таких полномочий общего характера, как проведение обыска и выемки, до специализированных методов, таких как сохранение компьютерных данных. Чаще всего в развитых странах используются полномочия общего характера (не специально предназначенные для киберпреступлений) в отношении всех следственных мероприятий[ii]:

- обыска компьютерного аппаратного обеспечения или компьютерных данных;
- выемки компьютерного аппаратного обеспечения или компьютерных данных;
- распоряжения о предоставлении информации о подписчиках, хранимых данных о потоках информации и содержании;
- сбора в режиме реального времени данных о потоках информации, о содержании данных;
- оперативного обеспечения сохранности компьютерных данных;

- использования удаленной компьютерно-технической экспертизы и трансграничного доступа к компьютерной системе или данным и др.

Многие страны заявляют об отсутствии юридических полномочий в отношении применения более «продвинутых» мер, таких как удаленная компьютерно-техническая экспертиза. Хотя традиционные процессуальные полномочия могут применяться в ситуациях, связанных с киберпреступлениями, во многих случаях такой подход может также привести к возникновению правовой неопределенности и поставить под сомнение законность сбора доказательств и их допустимость. В целом, национальные подходы к полномочиям по расследованию киберпреступлений менее единообразны, чем подход к криминализации многих киберпреступлений.

Независимо от правовой формы полномочий по проведению расследований органы используют право производства обыска и выемки для физического изъятия компьютерного оборудования и получения компьютерных данных. Большинство стран использует также распоряжения в целях получения хранимых компьютерных данных от поставщиков услуг Интернета. Однако, за исключением европейских стран, около одной трети государств сообщает о том, что третьи стороны в расследовании трудно заставить предоставлять информацию[i]. Особенно сложным является взаимодействие правоохранительных органов и поставщиков услуг Интернета. Последние располагают информацией об абонентах, о местоположении и содержании данных, счетами-фактурами, некоторыми журналами связи, информацией — все это может представлять собой важнейшие электронные доказательства совершения преступления. Обязательства, предусмотренные национальным законодательством, и политика в области хранения и раскрытия данных в частном секторе значительно различаются в зависимости от страны, отрасли и вида данных. Неофициальные отношения между правоохранительными органами и поставщиками услуг, о существовании которых сообщают более половины всех отмеченных в докладе ООН стран, помогают в процессе обмена информацией и укрепления доверия[i]. Это свидетельствуют о необходимости нахождения баланса между конфиденциальностью и соблюдением процессуальных норм, позволяющего своевременно раскрывать доказательства, с тем чтобы частный сектор не превратился в непреодолимое препятствие при проведении расследований[iii].

Расследование киберпреступлений неизменно сопряжено с необходимостью обеспечения неприкосновенности частной жизни в соответствии с положениями международного права в области прав человека. Согласно нормам в области прав человека, в законодательстве достаточно ясно должны быть изложены обстоятельства, при которых власти имеют право применять те или иные следственные действия, и должны существовать надлежащие и эффективные гарантии недопущения злоупотреблений. Национальное законодательство защищает право на неприкосновенность частной жизни, а также на ряд ограничений и гарантий в связи с проведением расследований. Однако в случае проведения транснациональных расследований возможны доступ к данным со стороны иностранных правоохранительных органов и потенциальные юрисдикционные пробелы в режимах защиты неприкосновенности частной жизни.

Киберпреступления носят транснациональный характер и связаны с вопросами проведения транснациональных расследований, суверенитета, юрисдикции, экстерриториальных доказательств и необходимостью международного сотрудничества. Киберпреступления приобретают транснациональный характер в том случае, если какой-либо элемент или существенное последствие преступления проявляются или часть преступления совершается на территории другой страны. Международное право предусматривает ряд оснований для юрисдикции в отношении таких деяний, в том числе различные виды юрисдикции по территориальному принципу и юрисдикции на основе гражданства. Некоторые из этих оснований закреплены в многосторонних документах по предупреждению киберпреступности.

Формы международного сотрудничества включают выдачу преступников, оказание взаимной правовой помощи, взаимное признание иностранных судебных решений и неофициальное сотрудничество между органами полиции различных стран. Ввиду неустойчивого характера электронных доказательств в рамках международного

сотрудничества в уголовных вопросах в области киберпреступности необходимо своевременное представление ответов и наличие возможности обращаться с просьбой о проведении специализированных следственных действий, таких как сохранение компьютерных данных. Время представления ответов в рамках официальных механизмов, согласно полученной информации, в случае просьб как о выдаче, так и об оказании взаимной правовой помощи — нескольких месяцев. Такой срок создает проблемы в деле сбора неустойчивых электронных доказательств.

Официальные и неофициальные каналы сотрудничества предназначены для регулирования процесса получения согласия государства на проведение иностранными правоохранительными органами расследований, затрагивающих суверенитет государства. Однако следователи, сознательно или бессознательно, все чаще обращаются к экстерриториальным данным в процессе сбора доказательств, не испрашивая согласия государства, в котором физически находятся эти данные. Эта ситуация возникает, в частности, с «облачными» компьютерными технологиями, предполагающими хранение данных в нескольких центрах в различных географических точках. Хотя «местонахождение» данных технически может быть установлено, оно приобретает все более искусственный характер, вплоть до того, что даже традиционные просьбы об оказании взаимной правовой помощи будут часто направляться в страну места нахождения поставщика услуг, а не страну, в которой физически расположен центр данных. Иностранные правоохранительные органы могут использовать прямой доступ к экстерриториальным данным в тех случаях, когда следователи используют существующее «живое» подключение с устройства подозреваемого или полученное законным образом разрешение на доступ к данным. Следователи правоохранительных органов иногда могут получать данные от экстерриториальных поставщиков услуг посредством неофициального прямого запроса, хотя поставщики услуг обычно требуют соблюдения надлежащей правовой процедуры. В соответствующих положениях о «трансграничном» доступе, содержащихся в Конвенции о киберпреступности Совета Европы, такие ситуации учитываются не в полной мере, поскольку упор в них делается на «согласие» лица, правомочного раскрывать данные, и предполагается, что место их нахождения известно в момент доступа к ним или их получения[iv].

В нынешней ситуации в области международного сотрудничества возникает риск образования группировок, в рамках которых существуют необходимые полномочия и процедуры для сотрудничества входящих в их состав стран, ограничивающихся по отношению ко всем другим странам «традиционными» видами международного сотрудничества, не учитывающими особенности электронных доказательств и глобальный характер киберпреступности. Это особенно касается сотрудничества при проведении расследований. Отсутствие общего подхода, в том числе в рамках существующих многосторонних договоров в области киберпреступности, означает, что могут возникать сложности при принятии таких мер, как оперативное обеспечение сохранности данных в странах, не входящих в число стран, имеющих международные обязательства в отношении обеспечения такого механизма и его задействования в случае поступления запроса. Включение таких полномочий в проект Конвенции ООН о кибербезопасности может в некоторой степени способствовать ликвидации этого пробела.

---

[i] http://www.unodc.org

[ii] http://www.un.org

[iii] http://ria.ru

[iv] http://www.conventions.coe.int