Проблемы расследования «Киберпреступности» в России

М.Г. Комаров
Прокурор управления по надзору за уголовно–процессуальной и оперативно–розыскной деятельностью прокуратуры Нижегородской области, юрист 1 класса

В условиях постоянного развития информационно–телекоммуникационных технологий и повсеместного использования компьютерной техники во всех сферах общественных отношений, отечественные правоохранительные органы оказались не в полной мере готовы эффективно противостоять новым видам преступных посягательств – киберпреступлениям.

Уголовный кодекс РФ не содержит указания, что именно следует понимать под «киберпреступлениями». Вместе с тем во многих источниках под этими преступлениями понимают: «компьютерные преступления», «преступления в сфере высоких технологий», «информационные преступления» и т.д. Независимо от используемой терминологии очевидно, что проблема борьбы с киберпреступлениями, является одной из приоритетных задач правоохранительных органов России.

За период 2014 года в России зарегистрировано более 11 000 компьютерных преступлений. Однако, по мнению экспертов, реальная цифра превышает указанное число в несколько раз.

По сведениям компании, занимающихся услугами компьютерной безопасности, количество взломов почты, с последующими негативными последствиями, исчисляется миллионами, а они также являются киберпреступлениями.

Самыми частыми киберпереступлениями, предусмотренными УК РФ являются: ст. 159.6 «Мошенничество в сфере компьютерной информации», ст. 242.1 «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации информационно–телекоммуникационных сетей», ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых,

телеграфных или иных сообщений», ст. 272 «Неправомерный доступ к компьютерной информации», ст. 137 «Нарушение неприкосновенности частной жизни», ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства».

По сведениям компании, занимающихся услугами компьютерной безопасности, количество взломов почты, с последующими негативными последствиями, исчисляется миллионами, а они также являются киберпреступлениями.

Такая ситуация стала возможна из–за того, что крайне редко подаются заявления в правоохранительные органы в случаях DDoS–атак, кражи логинов и паролей, а также установки вредоносных программ.

Кроме того, в 53% случаев с момента совершения преступления до поступления информации о совершенном преступлении проходит более 10 дней. Очевидно, что запоздалое начало предварительного расследования может привести к безвозвратной утрате важных доказательств, увеличению сроков предварительного расследования и другим негативным последствиям. Как правило, несвоевременное выявление киберпреступлений влечет за собой опасность уничтожения следов совершенного преступления

Другой сложностью эксперты называют слабое законодательство в России. Например, в США закон обязывает компании сообщать о такого рода атаках, а в России данной нормы нет, поэтому многие инциденты и остаются неизвестны правоохранительным органам.

Существенной проблемой расследования киберпреступлений является недостаточная компетентность лиц, которые занимаются их выявлением и раскрытием. Подавляющие большинство следователей и дознавателей имеет только юридическое образование, дополнительная подготовка, например специальность по «Информатике и вычислительной технике» ими получена не была.

Что касается компьютерно–технической экспертизы, то здесь надо отметить, что следователям приходится сталкиваться с загруженностью государственных судебно–экспертных учреждений и, как следствие, несвоевременностью выполнения экспертиз.

Таким образом, надо признать, что раскрытие и расследование киберпреступлений остается довольно сложной задачей для большинства сотрудников органов предварительного расследования. Это отчасти обусловлено отсутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов, а также недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях

Для решения данной проблемы, необходимо проведение обучения по расследованию данного вида преступлений, а также организация семинаров, посвященных модификации компьютерных технологий, а также совершенствование законодательства в том числе и на международном уровне.