Иванова Мария Михайлова
магистрант
Желудков Михаил Александрович
д-р юрид. наук, доцент, профессор
ФГБОУ ВО «Тамбовский государственный
технический университет»
г. Тамбов, Тамбовская область

ОТДЕЛЬНЫЕ ВОПРОСЫ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Аннотация*: актуальность изучения деятельности правоохранительных органов при расследовании и предупреждении киберпреступлений заключается в том, что эффективность подобного рода занятия невозможна без существенной методической и технической подготовки сотрудников, с учетом их постоянного профессионального обучения. Статья посвящена вопросам реализации организационно-технического обеспечения при расследовании преступлений в сфере компьютерных преступлений. Проведен анализ необходимых статистических данных, проанализирована деятельность соответствующих органов, занимающихся подобной деятельностью. Предложены рекомендации для решения отдельных вопросов повышения эффективности борьбы с киберпреступлениями.*

Ключевые слова*: компьютерная преступность, информационное общество, расследование киберпреступлений, профессиональная подготовка сотрудников, сотрудники правоохранительных органов.*

«Фундаментальной основой предупреждения преступности в России является Конституция Российской Федерации, где не только закреплены права и свободы человека и гражданина, но и выделены исходные положения защиты законных интересов личности, общества и государства. С учетом настоящего посыла предупреждение преступности должно нести в себе не только

воздействие на причины и условия конкретных преступлений, но и учитывать взаимосвязь различных видов и форм общественных отношений. Исторический опыт убедительно доказывает, что на первое место необходимо ставить не интересы государства и его правоохранительных структур, а идеологию защиты человека, прав и законных интересов личности» [3, с. 15–16].

На данном посыле с учетом специфики киберпреступности, при ее расследовании и предупреждении, специальное внимание следует уделять современным информационным технологиям, которые позволяют не только накапливать необходимую информацию, но и создают новые возможности, как для сотрудников правоохранительных органов, так и для кибер-преступников. Недаром современное общество имеет и свое название, а именно постиндустриальное или информационное общество [4, с. 881–885].

По статистике количество «пользователей сети на 2015 год позволяет выделить десять наиболее активных стран: Китай – 668 млн; Индия – 350 млн; США – 227 млн; Япония – 110 млн; Бразилия – 110 млн; Россия – 88 млн; Германия – 72 млн; Индонезия – 71 млн; Нигерия – 70 млн; Мексика – 59 млн» [10].

Как видим, в России данные технологии развиваются на уровне мировых стран, что несет за собой и развитие новых криминальных тенденций на высоком уровне. Современные преступники активно осваивают киберпространство, и постоянно совершенствуют новые средства и способы реализации киберпреступлений. «Социально-юридическая природа рассматриваемых поступков едина. Она определяется общей их социально-правовой характеристикой, местом в системе правовых явлений, выполняемыми функциями, что собственно и позволяет объединить их в единую систему» [6, с. 150].

В свою очередь, если обратить внимание на уголовное законодательство России, то оно в этом направлении развивается недостаточно быстро. Отметим, что: «Уголовный кодекс РФ не содержит указания, что именно следует понимать под «киберпреступлениями». Во многих источниках под этими преступлениями понимают: «компьютерные преступления», «преступления в сфере высоких технологий», «информационные преступления», «преступления в сфере

безопасности обращения компьютерной информации», «преступления в сфере компьютерной информации» и т.д.» [13].

Подобное положение «усугубляется отсутствием единообразного законодательного регулирования общественных отношений, связанных с использованием информационных ресурсов сети Интернет, как на национальном, так и на международном уровне» [5].

Отразим и тот факт, что: «принимая во внимание увеличение роли компьютерных информационных систем в жизни общества, масштабов их использования для обработки информации, популярность глобальной компьютерной сети Интернет и отсутствие готовности отечественных правоохранительных органов в полной мере эффективно противостоять новым видам преступных посягательств – киберпреступлениям, встает насущная проблема защиты от преступных посягательств, связанных с хищением, искажением или уничтожением компьютерной информации, неправомерным использованием компьютеров, а также умышленным нарушением их работы» [2].

Среди множества различных проблем таковой деятельности выделим моменты, связанные с определением правоохранительного органа, который должен стать координирующим центром при выявлении, раскрытии, расследовании и предупреждении киберпреступлений. В рамках его полномочий должно быть закреплено методическое совершенствование подобной деятельности и повышение надлежащей профессиональной подготовки сотрудников правоохранительных органов. Анализ нормативно-правового регулирования данной деятельности позволил выявить «пять основных элементов правоохранительной деятельности в области киберпреступлений – это полицейская доследственная работа, расследование преступлений, прокурорский надзор над следствием и оперативно-розыскной деятельностью (ОРД), гособвинение, суд» [8]. Подобная деятельность должна находиться под постоянным прокурорским надзором. «Следует обратить внимание, что при выявлении нарушений, прокурор должен добиваться их устранения, а при обнаружении признаков должностного правонарушения принимать

меры к привлечению виновных лиц к ответственности, в том числе уголовной» [9, с. 102].

Однако среди различного круга правоохранительных органов есть структура, которая непосредственно занимается борьбой и профилактикой киберпреступлений, а именно «Управление «К» Бюро специальных технических мероприятий МВД России». На сайте МВД России находим основные направления деятельности этой структуры:

«1. Борьба с преступлениями в сфере компьютерной информации:

1) выявление и пресечение фактов неправомерного доступа к компьютерной информации;

2) борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ;

3) противодействие мошенническим действиям с использованием возможностей электронных платежных систем;

4) борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет.

2. Пресечение противоправных действий в информационно - телекоммуникационных сетях, включая сеть Интернет:

1) выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи;

2) противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;

3) противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

3. Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

4. Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий.

5. Борьба с международными преступлениями в сфере информационных технологий:

1) противодействие преступлениям в сфере информационных технологий, носящим международный характер;

2) взаимодействие с национальными контактными пунктами зарубежных государств.

6. Международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий» [12].

Совокупность подобных направлений деятельности позволяет считать данную правоохранительную структуру среди тех, кто непосредственно находится на переднем крае борьбы с киберпреступлениями. Например: «В 2017 году сотрудники Управления «К» МВД России совместно с оперативниками отдела «К» МВД по Республике Татарстан пресекли деятельность лиц, осуществлявших хищения денег с банковских счетов граждан. В распоряжение оперативников поступила информация о том, что неизвестные лица создают в сети Интернет фишинговые страницы, полностью копирующие внешний вид популярных платежных систем, а также сервисов по продаже авиабилетов, и используют их в целях хищения денежных средств с банковских счетов и электронных кошельков граждан. Установлено, что фишинговые ресурсы позволили злоумышленникам получить платежные реквизиты большого количества пострадавших по всей стране и осуществить несанкционированные денежные переводы на заранее подготовленные банковские счета. Противоправная деятельность осуществлялась с 2015 года, а доход злоумышленников составлял порядка 1 миллиона рублей в месяц. В результате скоординированной операции, проведенной на территории Республики Татарстан и Краснодарского края, злоумышленников задержали. В ходе обысков обнаружены и изъяты компьютеры, на которые были установлены программные инструменты, использовавшиеся для осуществления противоправной деятельности, банковские карты. Возбуждено уголовное дело по признакам преступлений, предусмотренных ст. 272 и ст. 158 Уголовного кодекса

Российской Федерации. Задержанные дают признательные показания. В отношении фигурантов судом избрана мера пресечения в виде заключения под стражу» [7].

Даже по приведенному примеру видно, что раскрытие и расследование подобного вида преступности требует существенной методической и технической подготовки сотрудников, с учетом их постоянного профессионального обучения, что характерно не только для Российской Федерации. Так, «глава Интерпола Рэймонд Кендалл заявил, что резкий рост преступлений в сети застал полицию Европы врасплох. Нельзя просто взять констебля с улицы и научить его разбираться в высоких технологиях» [11].

«Опросы среди российских следователей показывают, что среди них 95% респондентов имеют юридическое образование. И только 5% обладают еще и дополнительным образованием по специальности «Информатика и вычислительная техника». 63% опрошенных владеют компьютером на уровне «среднего пользователя», 37% – на уровне «продвинутого пользователя». 79% при этом постигают компьютер самостоятельно, курсы для сотрудников правоохранительных органов посещали только 21%, и незначительный процент (5%) – коммерческие курсы» [13].

В субъектах Российской Федерации по настоящее время не создано специализированное следственное подразделение для непосредственно расследования только киберпреступлений. Следователи занимаются их расследованием совместно с другими общеуголовными деяниями. В то время как оперативные сотрудники из Управления «К» МВД России, обладая специальными познаниями, выявляют подобные деяния, следователи с неохотой берутся за их расследование. Сложности возникают уже на стадии выявления места преступления. «Примечательно, что 21% из числа опрошенных практических работников не проводили осмотр места происшествия по данным деяниям и отметили, что причиной отказа от проведения осмотра места происшествия является само отсутствие места происшествия» [1, с. 295].

Не менее актуальными остаются вопросы, возникающие перед следователем перед назначением экспертизы по киберпреступлениям. «Особую трудность при назначении подобной экспертизы вызывает процесс правильности постановки грамотных вопросов эксперту, проводящему компьютерно-техническую экспертизу. Назначающие экспертизу связывают возникающие трудности с отсутствием у них практики расследования данной категории дел, сложностью технических терминов и отсутствием специальных знаний в этой сфере» [1, с. 295].

На этой основе, современное организационно-техническое обеспечение борьбы с киберпреступлениями предполагает решение следующего круга задач:

1) повышение уровня мониторинга данного вида преступлений;

2) создание и внедрение в практику современных программ повышения квалификации следователей (дознавателей) по расследованию киберпреступлений;

3) насыщение технического обеспечения деятельности оперативных сотрудников и экспертов, специализирующихся в области исследования компьютерных технологий;

4) постоянное наполнение научно-методической литературой, посвященной прикладным аспектам расследования киберпреступлений [11].

Таким образом, получаемая сегодня сотрудниками правоохранительных органов, информация о киберпреступлениях содержит в себе массу всевозможных сведений, анализ которых позволяет максимально эффективно использовать полученные знания при расследовании преступлений и в оперативно-розыскных целях. Однако полученная информация не получит своего должного реагирования при отсутствии должного обеспечения профессиональной подготовки сотрудников, которые и будут ее облекать в процессуальную форму конкретного уголовного дела.

Список литературы

1. Аверьянова Т.В. Судебная экспертиза: Курс общей теории / Т.В. Аверьянова. – М.: Норма, 2006. – 480 с. [Электронный ресурс]. – Режим доступа: http://mylektsii.ru/11-59591.html/ (дата обращения 10.10.2017).

2. Белоусов А. Некоторые аспекты расследования компьютерных преступлений / А. Белоусов [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/library/Belous1106.html) (дата обращения 10.10.2017).

3. Желудков М.А. Соотношение принципов гуманизма и справедливости при реализации мер по предупреждению преступности [Текст] / М.А. Желудков // Проблемы правоохранительной деятельности. – 2016. – № 4. – С. 15–16.

4. Зверянская Л.П. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений / Л.П. Зверянская // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 881–885 [Электронный ресурс]. – Режим доступа: http://e-koncept.ru/2016/96090.htm. (дата обращения 10.10.2017).

5. Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг интернет / Д.А. Илюшин [Электронный ресурс]. – Режим доступа: http: // www.dslib.net/ kriminal-process / osobennosti-rassledovanija – prestuplenij -sovershaemyh -v-sfere-predostavlenija-uslug.html/ (дата обращения 10.10.2017).

6. Медведева С.В. Особенности классификации и состава обстоятельств, исключающих правовую ответственность личности [Текст] / С.В. Медведева, М.А. Ментюкова; Университет им. В.И. Вернадского // Вопросы современной науки и практики. – 2015. – № 1 (55). – С. 150.

7. Новости Управления «К» МВД РФ [Электронный ресурс]. – Режим доступа: https:// мвд.рф /mvd/ structure1/ Upravlenija/ Upravlenie_K_ MVD_Rossii /Publikacii_i_ vistuplenija/item/11078047/

8. Панеях Э. Правоохранительная деятельность в России: структура, функционирование, пути реформирования / Э. Панеях, А. Поздняков, К. Титаев, И. Четверикова, М. Шклярук [Электронный ресурс]. – Режим доступа: http://libed.ru/knigi-nauka/618657-1-pri-podderzhke-pravoohranitelnaya-deyatelnost-rossii-strukturafunkcionirovanie-puti-reformirovaniya-chast-per.php / (дата обращения 10.10.2017).

9. Печников Н.П. Проблемы теории и практики прокурорского надзора за процессуальной деятельностью органов предварительного следствия [Текст] / Н.П. Печников; Университет им. В.И. Вернадского // Вопросы современной науки и практики. – 2012. – №С38. – С. 102.

10. Статистика Интернета 2015 год [Электронный ресурс] // Режим доступа: http: //topolweb.ru/blog/statistics2015/ (дата обращения 10.10.2017).

11. Угланов Ю.А. Правовые и организационные вопросы борьбы с преступлениями в сфере компьютерной информации в российской федерации / Ю.А. Угланов [Электронный ресурс]. – Режим доступа: http://rudocs.exdat.com/docs/index-99869.html / (дата обращения 10.10.2017).

12. Управление «К» МВД России [Электронный ресурс]. – Режим доступа: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения 10.10.2017).

13. Шевченко Е.С. Актуальные проблемы компьютерных преступлений [Электронный ресурс] / Е.С. Шевченко. – Режим доступа: http:// stuchilin.ru / services/ r/ computer-crimes/311/ (дата обращения 10.10.2017).