УДК 378.046.4

НЕКОТОРЫЕ ВОПРОСЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СОТРУДНИКОВ СЛЕДСТВЕННОГО КОМИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Расчетов В.А., Бутенко О.С.

Первый факультет повышения квалификации (с дислокацией в городе Ростов-на-Дону) Института повышения квалификации ФГКОУ ВО «Академия Следственного комитета Российской Федерации», Ростов-на-Дону, ул. Волоколамская, 3в, e-mail: butenko_os@mail.ru.

В статье дается краткая характеристика основных аспектов криминалистического сопровождения расследования компьютерных преступлений, которые чаще всего становятся предметом рассмотрения в ходе повышения квалификации сотрудников Следственного комитета Российской Федерации. Приводится типолологизация лиц, совершающих компьютерные преступлений в зависимости от их мотивов и уровня знания компьютерной техники и программного обеспечения (в частности были выделены группы «хакеров», «крэкеров» и «временщиков»). Далее приводятся наиболее типичные следственные ситуации, которые сотрудники Следственного комитета Российской Федерации могут встретить на практике. Типичные следственные ситуации иллюстрируются примерами наиболее громких компьютерных преступлений последних лет. В заключении делается вывод о необходимости всестороннего повышения квалификации сотрудников СК России, а также необходимости теснейшего межведомственного взаимодействия при расследования сложных в техническом отношении компьютерных преступлений и преступлений, совершаемых с использованием компьютерной техники.

Ключевые слова: компьютерные преступления, отдельные следственные действия, повышение квалификации, криминалистическое сопровождение.

SOME QUESTIONS OF TRAINING STAFF INVESTIGATIVE COMMITTEE OF THE RUSSIAN FEDERATION IN INVESTIGATING COMPUTER CRIMES

Raschetov V.A., Butenko O.S.

The first advanced training faculty Institute for Advanced Studies of the Academy of the Investigative Committee the Russian Federation, Rostov-on-Don, ul. Volokolamsk, 3v, e-mail: butenko_os@mail.ru.

The article gives a brief description of the main aspects of forensic investigation of computer crime tracking, which often become the subject of consideration in the training of staff of the Investigative Committee of the Russian Federation. Provides classification of perpetrators of computer crime, depending on their motives and the level of knowledge of computer hardware and software (in particular were identified group "hackers", "crackers" and "temporary"). The following are the most typical investigative situations that officers of the Investigative Committee of the Russian Federation can meet in practice. Typical investigating the situation illustrated by examples of the most high-profile computer crimes in recent years. In conclusion, the conclusion about the necessity of comprehensive staff development of the Investigative Committee of the Russian Federation, as well as the need for close inter-agency cooperation in the investigation of technically complex computer crimes and crimes committed using computer technology.

Keywords: computer-related crime, the individual investigations, training, forensic support.

В современном мире в контексте активно идущих процессов информатизации общества, ведущую роль в развитии экономики и технологий играет обмен информацией. По мере развития компьютерных сетевых технологий, подключения к глобальным компьютерным сетям все большего количества пользователей, увеличивается угроза совершения компьютерных преступлений. Так, компания Cisco сообщает, что в 2013 году количество подключённых устройств к сети Интернет составило более 9 млрд [7], то есть на 2 млрд превысило общее количество жителей планеты Земля. Поэтому в современных условиях крайне актуальными становятся вопросы защиты информации, обеспечения

государственной, коммерческой и иной охраняемой законом тайны, а также выявление, раскрытие и расследование компьютерных преступлений. Все это ставит перед следователями Следственного комитета Российской Федерации новые требования, а задачей Академии Следственного комитета Российской Федерации является разработка курсов и программ повышения квалификации, которые бы в максимальной степени подготовили действующих сотрудников к расследованию компьютерных преступлений и преступлений, совершаемых с использованием компьютерной техники. В соответствии со статьёй 151 УПК РФ данные преступления относятся к непосредственной подследственности органов внутренних дел. Однако преступления указанной категории достаточно часто расследуются следователями Следственного комитета России (в силу возможности прокурора определять подследственность при соединении в одном производстве уголовных дел, подследственных разным органам предварительного расследования (п. 7 указанной статьи УПК РФ). Сказанное свидетельствует об актуальности рассмотрения данных преступлений в ходе повышения квалификации, поскольку у следователей СК России почти отсутствует практика расследования подобной категории дел. Далее нами будут рассмотрены основные аспекты, которые затрагиваются в ходе повышения квалификации сотрудников Следственного комитета Российской Федерации.

Для начала обратимся к вопросу о лицах, которые совершают компьютерные преступления. Данным вопросам посвящены достаточно обширные криминологические исследования последних лет (Вехов В.Б., Комиссаров В., Морар И.О., Осипенко А.Л., Россинская Е.Р., Шевченко Е.С.).

Как отмечает И.О. Морар, когда обращаются к типологизации лиц, совершающих те или иные виды преступлений, чаще всего выделяются следующие группы: так называемые «хакеры» (17 %) и «крэкеры» (32 %) и «временщики» (51 %).

Как отмечает И.О. Морар, «хакеры» и «крэкеры» осуществляют поиск уязвимых мест в компьютерных программах. Однако «хакер» при этом руководствуется желанием не только обнаружить слабые места в системе безопасности компьютерной системы, но и уведомить разработчиков и максимальное число пользователей, с целью минимизации возможного вреда и последующего устранения найденных недостатков, а также внесения предложений по усовершенствованию данной системы [5]. Поэтому термину «хакер», видимо, не всегда заслуженно придаётся сугубо негативный оттенок [1]. Хотя не вызывает сомнений то, что деятельность «хакера» имеет пограничный характер между правонарушением и требованиями закона. Все же его деятельность напоминает, скорее, некую игру, чем опасное преступное посягательство. Тем более, если при этом обратиться к основополагающим принципам российского уголовного законодательства, то в основе

квалификации преступлений, как хорошо известно, всегда должен лежать принцип субъективного, а не объективного вменения. Именно поэтому очень важно определить, какими целями руководствовалось лицо при взломе чьей-то компьютерной системы. Однако на практике это осуществить весьма не просто.

Деятельность «крэкера» имеет иные цели и задачи. При взломе компьютерной системы данное лицо стремится получить несанкционированный доступ к чужой информации, для использования её именно в своих, как правило, корыстных или иных преступных целях (месть, хулиганские побуждения, озорство, промышленный или иной вид шпионажа и пр.).

Группа «крэкеров» чаще всего также не является однородной и делится на три подгруппы:

1) «взломщики» – профессиональные «крэкеры», осуществляющие взлом компьютерных систем с целью хищений дорогостоящего программного обеспечения и денежных средств, а также промышленного и коммерческого шпионажа и т.д. Данная группа лиц обладает устойчивыми криминальными навыками. А совершаемые ими преступные посягательства, как правило, носят серийный характер. Профессиональный «крэкер» может действовать как в своих интересах, так и в интересах третьих лиц;

2) «вандалы» – целью данной категории преступников является взлом компьютерной системы для её последующего разрушения;

3) «шутники» имеют целью незаконное внедрение в действующую компьютерную программу различных звуковых и/или визуальных эффектов.

И наконец, кроме отмеченных категорий правонарушителей, существенную по численности группу составляют так называемые «временщики», не обладающие серьёзными познаниями в соответствующей сфере, но их деятельность также направлена на уничтожение, блокирование или изменение плохо защищённой информации [7].

Кроме того, исследователи выделяют **три** наиболее часто встречающиеся **типичные следственные ситуации** при расследовании компьютерных преступлений.

Первая типичная следственная ситуация. Собственник информационной системы собственными силами выявил нарушение целостности или конфиденциальности информации, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

В качестве примера такой ситуации можно привести историю одного из первых хакеров в мире – Кевина Митника, который ночью 25 декабря 1994 года взломал домашний компьютер Цутому Симомуры, ведущего американского специалиста по компьютерной безопасности Агентства национальной безопасности США. В результате атаки хакер успешно скопировал сотни засекреченных файлов. Поймать Митника стало для Симомуры

делом чести, ведь факт взлома подрывал его профессиональную репутацию, а кроме того, помимо украденных файлов он нашёл на своём компьютере звуковое послание, в котором Митник оскорблял Симомуру. Для поимки хакера потребовалось достаточно продолжительное время, и в феврале 1995 года Митник был арестован. Ему было предъявлено 23 обвинения в мошенничестве с использованием компьютерных систем. Митнику инкриминировались деяния, повлёкшие причинение вреда на сумму, превышающую 80 миллионов долларов. Усилиями адвокатов большинство обвинений было снято и назначено наказание – 11 месяцев лишения свободы, запрет на следующие три года приближаться к любым компьютерным устройствам. Видимо суд внял доводам защиты, что все взломы Митник осуществлял просто из интереса.

Вторая типичная следственная ситуация. Собственник информационной системы собственными силами выявил нарушение целостности или конфиденциальности информации в системе, но не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

Но не всегда хакеры настолько альтруистичны. В последние годы сетевые компьютерные преступления совершаются, как правило, организованными преступными группами, часто общающимися между собой только посредством сети Интернет, при этом члены группы могут находиться в разных странах. Кроме того, вред, причинённый в результате преступных действий, характеризуется, как правило, крупным и особо крупным размером. Учитывая, что преступниками используются глобальные компьютерные сети, преступления могут совершаться на значительном расстоянии, в том числе с выходом за пределы национальных границ государств. Поэтому для пресечения деятельности таких группировок требуются совместные усилия служб безопасности разных государств, а при расследовании преступлений возникает необходимость в совершении следственных и иных процессуальных действий на территории нескольких государств.

Одним из наиболее актуальных и ярких примеров проявления киберпреступности является RedOctober – серия кибератак, которые происходили как минимум на протяжении последних шести лет. В 2013 году информацию о раскрытии этой сети кибершпионажа сообщили специалисты лаборатории Касперского. В рамках серии операций RedOctober были атакованы организации по всему миру.

В рамках шпионажа собирались данные и секретная информация с мобильных устройств, компьютеров и сетевого оборудования атакованных организаций. Основной целью операции, как отмечают специалисты лаборатории Касперского, является сбор секретной информации и геополитических данных.

Особенностью данных атак было, во-первых, крайняя индивидуализация каждой

атаки, использование данных, полученных от предыдущих атак (логинов, паролей, ID) и управление заражением дистанционно с анализом, поступающим от различным модулей вредоносной программы, а во-вторых, высокая скрытность деятельности злоумышленников, позволившая им оставаться незамеченными более 5 лет.

Таким образом, были похищены сотни терабайт информации, в том числе относящейся к категории охраняемой законом тайны. Расследование деятельности RedOctober в настоящее время продолжается.

Третьей типичной следственной ситуацией является такая, когда данные о нарушении целостности или конфиденциальности информации в информационной системе и виновном лице стали общеизвестными или непосредственно обнаружены правоохранительными органами (например, в ходе проведения оперативно-розыскных мероприятий).

К этой группе чаще всего относятся мошенничества с использованием компьютерных технологий. В отчёте компании Group-IB, которая специализируется в области компьютерной безопасности и достаточно тесно сотрудничает с органами, осуществляющими предварительное расследование и оперативно-розыскные мероприятия, приводится пример пресечения деятельности преступной группы Carberp, которая много лет специализировалась на хищениях в системах дистанционного банковского обслуживания.

Из материалов отчёта следует, что вредоносная программа Carberp была создана в 2008 году. Изначально она разрабатывалась как программа-загрузчик, однако автор начал наращивать функционал, постепенно добавляя различные грабберы (программы, которые извлекают из чужого сайта или программы важные сведения и передают их хозяину граббера), что в итоге превратило Carberp в технологичный банковский троян.

В 2009 году программой заинтересовался один из российских киберпреступников. Связавшись с автором трояна напрямую, злоумышленник (мужчина 1987 года рождения) организовал преступную группу, осуществлявшую посредством Carberp хищения у клиентов банков через системы дистанционного банковского обслуживания. За годы своей деятельности киберпреступники совершили хищения у тысяч юридических лиц практически во всех регионах России и более 100 банков.

Внимание правоохранительных органов обратилось на эту преступную группу в 2010 году. В ходе проведения оперативно-розыскных мероприятий и предварительного расследования было установлено, что для совершения хищений в 2009 и начале 2010 года злоумышленники использовали только программу Carberp, которая копировала ключи электронно-цифровой подписи, перехватывала пароли и делала снимки экранов во время работы пользователей с системой дистанционного банковского обслуживания. Этой

информации было достаточно для перевода денежных средств из любой точки мира.

Во второй половине 2012 года организатор преступной группы решил увеличить объёмы совершения хищений и привлёк для этого двух сообщников (братьев 29 и 26 лет, проживавших в Москве). Их задачей было обеспечение регулярного обналичивания денежных средств, а также привлечение новых участников в данную преступную группу. Младший из братьев уже имел богатый криминальный опыт и на тот момент находился в федеральном розыске за мошенничество с недвижимостью.

Количество потенциальных потерпевших юридических и физических лиц, на компьютерах которых были установлены вредоносные программы, используемые для хищения, быстро росло. Злоумышленники в текущем составе уже не успевали проверять счета и отслеживать движения денежных средств по ним, совершать хищения, открывать компании для вывода денежных средств и привлекать все новых сообщников. Чтобы распределить нагрузку, они расширяли состав преступной группы, привлекая новых участников, которые брали на себя работу по ручной проверке счетов и формированию поддельных платёжных поручений.

Эффективность преступной деятельности злоумышленников была настолько высока, что для комфортной работы руководителями преступной группы был открыт офис, который функционировал под видом компании по восстановлению данных. Позднее при обыске в офисе этой фирмы сотрудники МВД нашли большое число банковских карт, бланков различных документов, поддельные печати, а также 7,5 миллионов рублей наличными.

14 марта 2012 года подразделениями ФСБ и МВД России при участии специалистов Group-IB участники организованной преступной группы Carberp (8 человек) были задержаны. Задержание проходило одновременно в двух регионах России, что позволило избежать информирования остальных участников и пресечь возможности уничтожения доказательств.

В результате успешно проведённой операции преступная группа была ликвидирована. Впервые в российской практике удалось установить всю преступную цепочку, включая организатора группы, «заливщиков», проводящих мошеннические операции, и «дропов» – лиц, непосредственно осуществляющих обналичивание похищенных денежных средств. По результатам расследования Сбербанк России возместил убытки всем физическим лицам, пострадавшим от действий преступной группы.

Таким образом, мы рассмотрели основные следственные ситуации, с которыми может столкнуться в своей практике следователи Следственного комитета Российской Федерации. Актуальность изучения вопросов расследования компьютерных преступлений в рамках повышения квалификации сотрудников Следственного комитета Российской Федерации

обуславливается тем, что компьютерные преступлений отличаются сложностью и латентностью, и для выявления противоправности действий преступника, и поиска следов компьютерного преступления требуются совместные усилия следователя, оперативных работников и экспертов, обладающих опытом и глубокими знаниями в области электронной техники и информационных технологий. Без тесного взаимодействия правоохранительных органов привлечение лица к уголовной ответственности, даже при наличии признаков состава преступления, становится проблематичным.

Кроме того, повышение эффективности расследования компьютерных преступлений и уголовного преследования по таким делам все в большей степени становится зависимым от высокой профессиональной подготовки следователей, оперативных работников, прокуроров, судей.

Список литературы

1. Айков Д., Сейгер К., Фонстрох У. Компьютерные преступления. М., 1999. С. 91.
2. Берлявский Л.Г., Расчетов В.А. Следственный комитет Российской Федерации: конституционно-правовые основы организации и деятельности // Российский следователь. 2014. № 5. С. 52-55.
3. Бутенко О.С. «Теоретические и практические аспекты международного сотрудничества в ходе уголовного судопроизводства» // Научная мысль Кавказа. 2012. № 3 (71). С. 111-113.
4. Косынкин А.А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования [Текст] / А. А. Косынкин // Рос. следователь. 2012. № 2. С. 2-3.
5. Морар И.О. Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления // Российский следователь. 2012. № 13.
6. Осипенко, А.Л. Особенности расследования сетевых компьютерных преступлений [Текст] /А. Л. Осипенко // Российский юридический журнал. 2010. № 2. С. 121–126.
7. Отчет о безопасности компании Cisco за 2013 год http://www.cisco.com/web/RU/downloads/broch/Cisco_Annual_Security_Report_2013_RU.pdf

Рецензенты:

Федотова О., д.п.н., профессор, заведующая кафедрой образования и педагогических наук Академии психологии и педагогики Южного федерального университета, г. Ростов-на-Дону.

Сафонцев С.А., д.п.н., профессор, профессор кафедры образования и педагогических наук

Академии психологии и педагогики Южного федерального университета, г. Ростов-на-Дону.