УДК 343.9

О.А. Егерева
В.В. Коломинов
М.С. Сизова

НЕКОТОРЫЕ ВОПРОСЫ МЕТОДИКИ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

В статье авторы делают акцент на распространенности и серьезности угрозы киберпреступлений. Расследование киберпреступлений определяет необходимость производства множества следственных действий. Поскольку расследование данных преступлений требует специфических знаний в области компьютерных технологий, которыми на должном уровне не всегда обладает следователь, к следственным действиям привлекают специалистов в данной области знаний. Авторы приводят аргументы в пользу преимущественного использования специальных знаний при проведении ряда следственных действий. Отмечается роль элементов, касающихся компьютерной информации, компьютерных средств, механизма следообразования в формировании криминалистического знания при расследовании киберпреступлений.

Ключевые слова: киберпреступность, компьютерные преступления, киберпреступность, осмотр, допрос, компьютерно-техническая экспертиза.

O.A. Egereva
V.V. Kolominov
M.S. Sizova

SOME QUESTIONS OF THE TECHNIQUE OF THE INVESTIGATION OF CYBER CRIMES

In the article, the authors focus on the prevalence and severity of the threat of cybercrime. The investigation of cybercrime determines the need for a variety of investigative actions. Since the investigation of these crimes requires specific knowledge in the field of computer technology, which the investigator does not always possess at the proper level, experts in this field of knowledge are attracted to investigative actions. The authors argue in favor of the preferential use of special knowledge in a number of investigative actions. The role of elements relating to computer information, computer tools, the mechanism of trace in the formation of forensic knowledge in the investigation of cybercrime is noted.

Keywords: cybercrime, computer crimes, cybercrime, inspection, interrogation, computer-technical expertise.

Каждый день во всем мире происходят десятки тысяч инцидентов, связанных с информационной безопасностью. Перечень таких инцидентов достаточно широк. Условно их можно объединить в две группы: внутренние (компрометация данных, утечка конфиденциальной информации, аномальная сетевая активность, и т.д.) и внешние (фишинг, кардинг, DDoS-атаки («Отказ в обслуживании»), целевые атаки и т.д.).

Согласно представленному отчету «NORTON REPORT 2017» международной корпорацией Symantec[1], ущерб от компьютерных преступлений во всем мире оценивается в 113 млрд дол. США. По оценкам другой авторитетной международной компаний по предотвращению и расследованию киберпреступлений «Group-IB» в России и СНГ за 2016–2017 г. совершено хищений на сумму 2,5 млрд дол. США, что составляет 2% от глобального рынка, оцененного корпорацией Symantec. Отмечается активный рост хищений со счетов российских банков с использованием зараженных мобильных устройств. За период с третьего квартала 2016 г. по второй квартал 2017 г. было выявлено 5 организованных преступных групп, использующих уникальное вредоносное программное обеспечение. Компанией Group-IB было зафиксировано множество целевых атак на финансовые организации, которые завершились успешным проникновением злоумышленников извне во внутренние сети, а также получением доступа к банковским и платежным системам[2].

Безусловно, такие явления требуют немедленного реагирования правоохранительных органов. Основная масса киберпреступлений расследуются Управлением «К» МВД России и региональными структурными подразделениями, а также специализированными подразделениями ФСБ России. Особое значение, как отметил В.В. Путин на заседании коллегии ФСБ России, имеют случаи, когда затрагиваются интересы национальной информационной безопасности государства [1, с. 166]. Так, в 2017 г. было пресечено около 74 млн кибератак на официальные сайты и информационные системы органов власти [1, с. 167].

---

[1] Официальный сайт LETA IT-company. URL: http://www.leta.ru/services/cybercrime-investigation/cybercrime-laboratory.html (дата обращения: 26.04.2015 г.).

[2] Официальный сайт Group-IB. URL: http://www.group-ib.ru/index.php/kriminalistika/79-link-investigation (дата обращения: 26.04.2015 г.).

Как правило, поводом возбуждения уголовного дела являются заявления о несанкционированном доступе, хищении денежных средств. Поступают они от организаций, намного реже от граждан. Объяснением этому может быть то, что граждане бояться разглашения в ходе следствия украденной информации, которая может содержать тайные, интимные и иные подробности личной жизни. Поэтому при возникновении подобной ситуации следователю необходимо наладить психологический контакт, объяснить гражданину, что следствие интересуют только те данные, которые имеют значение для расследования преступления и не могут быть разглашены третьим лицам.

Первоначально необходимо провести неотложные следственные действия, связанные со сбором вещественных доказательств, например, осмотр места происшествия, который неразрывно связан с осмотром компьютера, периферийного оборудования и иных объектов. Практически вся следовая информация хранится в памяти компьютера, поэтому особое внимание следует уделять осмотру машинных носителей. Необходимо учитывать и то, что существует угроза потери данных указанных объектов, поэтому в этом случае целесообразно их изымать для последующего исследования в лабораторных условиях в рамках компьютерной технической экспертизы.

При допросе заявителя-потерпевшего следователь подробно получает и фиксирует в протоколе информацию, а именно о совершенных за последние 3–4 дня компьютерных операциях, действиях: какая сумма была украдена, какие сайты посещались, какие программы (приложения) были установлены и т.д. При этом следователь должен исключить возможность инсценировки преступления, что бывает достаточно часто на практике, путем постановки дополнительных вопросов, изучением личности потерпевшего, установлением наличия

профессиональных знаний в области информационных технологий у допрашиваемых лиц и назначением экспертизы [2, с. 131].

Назначение компьютерно-технической экспертизы имеет огромное значение для сбора доказательственной информации. Для этого эксперту необходимо предоставить материалы для сравнительного исследования, объекты, изъятые в ходе осмотра места происшествия, которые были упомянуты выше. Если предоставить устройства на исследование эксперту не представляется возможным, то следователю целесообразно делать копию жесткого диска на месте совершения преступления, например, в организации. Для таких мероприятий существует криминалистический дубликат - разработка российских ученых, которая позволяет с идентичностью снять копию с любого цифрового устройства [3, с. 131]. Самостоятельно следователю в виду недостаточных знаний будет достаточно сложно или вовсе невозможно правильно изъять копию, поэтому тактически целесообразно при проведении всех следственных действий, как на первоначальном, так и последующих этапах расследования, привлекать специалиста в области компьютерной информации и компьютерной техники.

Конечно, привлекать квалифицированных специалистов по таким категориям дел не всегда представляется возможным по экономическим соображениям и узконаправленной сферой специализации. Тем не менее, многие крупные компании, банки и другие учреждения, где проходят большие обороты финансовых средств в электронной среде, заключают договоры на оказание услуг по предотвращению и расследованию киберпреступлений с авторитетными специализированными организациями, такими как Group-IB[1] и LETA

[1] Официальный сайт Group-IB. URL: http://www.group-ib.ru/index.php/kriminalistika/79-link-investigation (дата обращения: 26.04.2015 г.).

IT-company[1], деятельность которых осуществляется не только в России, но и в других странах. Данные организации в своем штате имеют высококвалифицированных специалистов, криминалистические лаборатории, оборудование и готовы оказывать содействие правоохранительным органам. Безусловно, такое сотрудничество, обмен опытом передовых технологий в разы позволяет эффективнее расследовать компьютерные преступления.

В ходе компьютерно-технической экспертизы будут исследованы системные и программные файлы на наличие несанкционированного доступа, аномальная сетевая активность, время начала и окончания атак, типы, характеристика. Огромное значение для экспертов имеют лог-файлы (файлы расширения .log). Лог-файлы представлены в виде текстовой информации, которые хранят историю о всех интернет соединениях, исходящих и входящих запросах на компьютер потерпевшего. В лог-файлах будут так же перечислены IP-адреса, с которых производились запросы к серверу, устройству потерпевшего. По результатам экспертизы следователю предстоит выполнить огромную работу совместно с оперативными сотрудниками путем проведения следственных действий и оперативно-розыскных мероприятий по установлению принадлежности IP-адресов к конкретным лицам [4, с. 63]. Например, это могут быть запросы к хостинг-провайдерам о предоставлении данных о владельце IP-адреса (сервера), которые обслуживаются данным провайдером. При регистрации серверов владельцы указывают данные, в основном это номер телефона, почтовый адрес, адрес места жительства, однако некоторые хостинг-провайдеры в своей политике безопасности требуют указывать и паспортные данные, что упростит процедуру идентификации пре-

[1] Официальный сайт LETA IT-company. URL: http://www.leta.ru/services/cybercrime-investigation/cybercrime-laboratory.html (дата обращения: 26.04.2015 г.).

ступника. К сожалению, в России преимущественно используются динамические IP-адреса, намного реже статические. Так один динамический IP-адрес может принадлежать 10, 100, 1000 клиентам, что существенно затрудняет поиск злоумышленника.

Эксперту предстоит проделать кропотливую работу тогда, когда имеются признаки заражения компьютера (планшета, смартфона) трояном, вирусом-шпионом и прочими вредоносными программами. Как показывает практика, в 86 % случаев на зараженных устройствах было установлено антивирусное программное обеспечение [5]. Поэтому эксперту предстоит буквально вручную отыскать вредоносный код (скрипт) путем декомпиляции всех установленных программ, что требует значительного количества времени. Так, например, при заражении смартфона с предустановленной операционной системой «Android» будут исследоваться подозрительные приложения (файлы расширения .apk формата). При исследовании вредоносного кода (скрипта) эксперт обнаружит в части кода IP-адрес, на который несанкционированно троян отправляет скомпрометированную информацию. Остается определить принадлежность IP-адреса лицам по вышеописанной схеме.

Путем дальнейших оперативно-розыскных мероприятий необходимо установить местонахождения предполагаемого преступника и провести его задержание. Следователю по месту жительства злоумышленника следует организовать и провести обыск (выемку), в результате чего будет собрана доказательственная информация, которая будет положена в основу обвинения, а также провести иные следственные действия. Поскольку следственные действия предоставляют в определенных рамках возможность выбора варианта и стратегии поведения следователя [6, с. 16].

Таким образом, качественно проведенные первоначальные следственные действия и оперативно-розыскные мероприятия, своевре-

менный сбор доказательственной информации с привлечением высококвалифицированных специалистов, назначение экспертиз влияют на результат, от которого будет зависеть эффективность предотвращение и расследование компьютерных преступлений.

Список использованной литературы

1. Харина Э.Н. Киберпреступность: уголовно-правовой и криминалистический аспект / Э.Н. Харина // Вестник Университета имени О.Е. Кутафина. – 2017. – № 5. – С. 164–171.

2. Харина Э.Н. О возможностях использования сети Интернет при расследовании преступлений / Э.Н. Харина // Современное состояние и перспективы развития научной мысли : материалы Междунар. науч.-практ. конф., г. Уфа, 25 мая 2015 г. : в 2 ч. – Уфа : Аэтерна, 2015. – Ч. 2. – С. 131–132.

3. Россинская Е.Р. Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. – М. : Право и закон, 2001. – 414 с.

4. Россинская Е.Р. Судебная компьютерно-техническая экспертиза: проблемы становления и подготовки кадров экспертов / Е.Р. Россинская // Теория и практика судебной экспертизы. – 2008. – № 3. – С. 60–66.

5. Россинская Е.Р. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем / Е.Р. Россинская, Г.П. Шамаев // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). – 2015. – Т. 6, № 1. – URL : http://brj-bguep.ru/reader/article.aspx?id=19969.

6. Низамов В.Ю. Производство следственных действий в условиях взаимодействия следователя и органа, осуществляющего оперативно-розыскную деятельность : учеб.-практ. пособие / В.Ю. Низамов, Д.А. Степаненко. Иркутск : Изд-во БГУЭП, 2004. 169 с.

Информация об авторах

Егерева Олеся Александровна – доцент, кафедра криминалистики, судебных экспертиз и юридической психологии Института государства и права, Байкальский государственный университет, 664003, г. Иркутск, ул. Ленина, 11; e-mail: olirk@mail.ru

Коломинов Вячеслав Валентинович – доцент, кафедра криминалистики, судебных экспертиз и юридической психологии Института государства и права, Байкальский государственный университет, 664003, г. Иркутск, ул. Ленина, 11; e-mail: OffRoad88@mail.ru.

Сизова Маяй Сергеевна – старший преподаватель кафедры криминалистики, судебных экспертиз и юридической психологии Института государства и права, Байкальский государственный университет, 664003, г. Иркутск, ул. Ленина, 11; e-mail: ms-pochta@mail.ru.

Information about the authors

Olesya A. Egereva – PhD of Law, Associate Professor, Chair of Criminalistics, Judicial Examinations and Legal Psychology of Institute of State and Law, Baikal State University, 11 Lenin Str., 664003, Irkutsk, Russian Federation; e-mail: olirk@mail.ru.

Vycheslav V. Kolominov – PhD of Law, Associate Professor, Chair of Criminalistics, Judicial Examinations and Legal Psychology of Institute of State and Law, Baikal State University, 11 Lenin Str., 664003, Irkutsk, Russian Federation; e-mail: OffRoad88@mail.ru.

Mayya S. Sizova – Senior Lecturer, Chair of Criminalistics, Judicial Examinations and Legal Psychology of Institute of State and Law, Baikal State University, 11 Lenin Str., 664003, Irkutsk, Russian Federation; e-mail: ms-pochta@mail.ru.