КРИМИНОЛОГИЯ И КРИМИНАЛИСТИКА

УДК 343.98
DOI: 10.54649/2077-9860-2023-3-13-18

К.Б. Брушковский[1]
[1]к.ю.н., ассоциированный профессор,
Каспийский общественный университет,
Республика Казахстан, г. Алматы
E-mail: brushkovskiy@mail.ru

ФОРЕНЗИКА – КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

Аннотация

В статье рассматриваются вопросы о раскрытии преступлений, связанных с компьютерной информацией, об исследовании доказательств в виде компьютерной информации, методах поиска, получения и закрепления таких доказательств.

Автор дает понятие «форензика» и раскрывает ее актуальность на сегодняшний день. Он отмечает, что форензика актуальна при расследовании не только компьютерных преступлений, дел об авторских правах на продукты, представленные в электронном виде, о доменных именах и др. средствах индивидуализации в Интернете, но также и других видов преступлений, непосредственно не являющихся компьютерными, но имеющих цифровые следы. Также показаны сферы применения форензики, криминалистическая характеристика, этапы криминалистического процесса.

Ключевые слова: форензика, компьютерная криминалистика, расследование киберпреступлений, борьба с преступностью, специалист, эксперт, хакер, научная лаборатория, современная техника.

К.Б. Брушковский1
[1]з.ғ.к., қауымдастырылған профессор,
Каспий қоғамдық университеті,
Қазақстан Республикасы, Алматы қ
E-mail**:** brushkovskiy@mail.ru

ФОРЕНЗИКА – КОМПЬЮТЕРЛІК КРИМИНАЛИСТИКА

Аңдатпа

Мақалада компьютерлік ақпаратпен байланысты қылмыстарды ашу, компьютерлік ақпарат түріндегі дәлелдемелерді зерттеу, мұндай дәлелдемелерді іздеу, алу және қамтамасыз ету әдістері қарастырылған.

Автор «форензика» ұғымын беріп, оның бүгінгі күнгі өзектілігін ашады. Ол форензиканың тек компьютерлік қылмыстарды ғана емес, электронды түрде ұсынылған өнімдерге, домендік атауларға және Интернетте дараландырудың басқа құралдарына авторлық құқықты қорғау істерін ғана емес, сонымен қатар тікелей компьютерлік қылмыс болып табылмайтын, сандық іздері бар қылмыстардың басқа да түрлерін тергеуде маңызды екенін атап өтеді. Сондай-ақ форензика қолданылу аясы, криминалистикалық сипаттамасы, криминалистикалық процестің кезеңдері көрсетілген.

Түйінді сөздер: форензика, компьютерлік криминалистика, киберқылмыстарды тергеу, қылмыспен күрес, маман, сарапшы, хакер, ғылыми зертхана, заманауи техника.

K.B. Brushkovskiy[1]
[1]candidate of law sciences, associate professor,
Caspian Public University,
Republic of Kazakhstan, Almaty
E-mail**:** brushkovskiy@mail.ru

FORENSICS - COMPUTER CRIMINALISTICS

Annotation

The article discusses issues of solving crimes related to computer information, the study of evidence in the form of computer information, methods of searching, obtaining and securing such evidence.

The author gives the concept of "forensics" and reveals its relevance today. He notes that forensics is relevant in the investigation of not only computer crimes, cases of copyright for products presented in electronic form, domain names and other means of individualization on the Internet, but also other types of crimes that are not directly computer crimes, but have digital traces. The scope of application of forensics, forensic characteristics, and stages of the forensic process are also shown.

Key words: forensics, computer criminalistics, investigation of cybercrimes, fight against crime, specialist, expert, hacker, scientific laboratory, modern technology.

Термин «форе́нзика» произошел от латинского «foren», что значит «речь перед форумом», то есть выступление перед судом, судебные дебаты. Термин «forensics» является сокращенной формой «forensic science», дословно «судебная наука», то есть наука об исследовании доказательств – именно то, что в русском именуется криминалистикой. Соответственно, раздел криминалистики, изучающий компьютерные доказательства, называется по-английски «computer forensics». При заимствовании слово сузило свое значение. Русское «форензика» означает не всякую криминалистику, а именно компьютерную.

Форензика (компьютерная криминалистика, расследование киберпреступлений) — прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств. Форензика является подразделом криминалистики, и решает:

1) разработка тактики ОРМ и следственных действий, связанных с компьютерной информацией;

2) создание методов, аппаратных и программных инструментов для сбора и исследования доказательств компьютерных преступлений;

3) установление криминалистических характеристик правонарушений, связанных с компьютерной информацией.

Сегодня форензика актуальна при расследовании не только компьютерных преступлений, дел об авторских правах на продукты, представленные в электронном виде, о доменных именах и др. средствах индивидуализации в Интернете, но также и других видов преступлений, непосредственно не являющихся компьютерными, но имеющих цифровые следы.

Среди таких преступлений необходимо отметить:

-терроризм;

-детскую порнографию;

-кражи;

-уничтожение объектов интеллектуальной собственности;

-финансовые преступления; преступления против коммерческой тайны;

-преступления с недвижимостью;

-мошенничество и др.

Сферы применения:

1. Раскрытие и расследование уголовных преступлений, в которых фигурируют компьютерная информация как объект посягательства, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства.

2. Сбор и исследование доказательств для гражданских дел, когда такие доказательства имеют вид компьютерной информации. Особенно это актуально по делам о нарушении прав интеллектуальной собственности, когда объект этих прав представлен в виде компьютерной информации – программа для ЭВМ, иное произведение в цифровой форме, товарный знак в сети Интернет, доменное имя и т.п.

3. Страховые расследования, проводимые страховыми компаниями касательно возможных нарушений условий договора, страхового мошенничества, особенно ко да объект страхования представлен в

виде компьютерной информации или таким объектом является информационная система.

4. Внутрикорпоративные расследования инцидентов безопасности, касающихся информационных систем, а также работы по предотвращению утечки информации, содержащей коммерческую тайну и иные конфиденциальные данные.

5. Задачи по защите гражданами своей личной информации в электронном виде, самозащиты своих прав, когда это связано с электронными документами и информационными системами.

Криминалистическая характеристика включает следующее:

– способ совершения преступления, предмет посягательства;

–личность вероятного преступника и вероятные его мотивы;

–личность вероятного потерпевшего;

– механизм образования следов

– обстановка и другие типичные обстоятельства образования

Личность вероятного преступника. Оценивая вероятного преступника, важнее всего для нас установить уровень его компетенции в области ИТ. Этот параметр является критическим. В технических методах борьбы, в соревнованиях «спрятать-найти» или «стереть-восстановить» уровень специальных знаний является решающим.

«Хакер» (наименование условное). Основной мотивацией этого типа нарушителей являются: исследовательский интерес, любопытство, стремление доказать свои возможности, честолюбие. Средства защиты компьютерной информации, ее недоступность они воспринимают как вызов своим способностям. Некоторые исследователи полагают необходимой чертой этого типа хорошие знания в области ИТ и программирования.

Е-бизмесмен (наименование условное). Этот тип вероятного преступника не является квалифицированным ИТ специалистом и не имеет служебного положения, которым можно злоупотребить. С самого начала он планирует именно криминальное предприятие, отлично осознаёт его противозаконность. Решение совершить правонарушение именно в компьютерной (сетевой) среде, а не в офлайне он принял не из-за своих особых знаний в этой области и не из-за внутренней тяги к компьютерам, а исключительно на основе рационального анализа, так будет выгоднее.

«*Инсайдер» (наименование условное).* Несколько более распространенным типом компьютерного злоумышленника является человек, не слишком хорошо владеющий знаниями в области ИТ, зато владеющий доступом в информационную систему в силу служебного положения. Уже стало общим местом утверждение, что большая часть «взломов» компьютерных систем совершается изнутри. Поэтому при расследовании неправомерного доступа «инсайдер» - первая версия, которую следует рассматривать. Даже если неправомерный доступ был явно снаружи, скорее всего, он стал возможным из-за сговора с местным сотрудником.

«*Белый воротничок» (наименование условное).* Этот тип преступника представляет собой давно и хорошо известного казнокрада, но только сменившего инструменты своей деятельности на компьютер. Кроме хищения здесь возможны взятки, коммерческий подкуп, незаконное использование информации, составляющей коммерческую тайну, различные виды мошенничества и так далее. В отличие от «инсайдера», этот тип злоумышленника имеет минимальную квалификацию в сфере ИТ и компьютер как орудие совершения преступления не использует. Компьютер здесь выступает только как носитель следов, доказательств совершения преступления.

По своим мотивам «белые воротнички» могут быть разделены *на три группы:*

1. Злоупотребляющие своим служебным положением из чувства обиды на компанию или руководителей. Их следует искать среди долго проработавших сотрудников. Причем для возникновения мотива мести совсем не обязательно наличие действительной обиды со стороны работодателя. В значительной части случаев, как отмечалось выше, обиды эти оказываются вымышленными. Такой обиженный, обойденный и недостойно оплачиваемый злоумышленник чаще всего ворует, чтобы «компенсировать» якобы недополученное от работодателя. Но бывают и бескорыстные мстители, которые не приобретают выгоды от своих незаконных действий либо по этическим соображениям (реже), либо для снижения вероятности раскрытия преступления (чаще).

2. Беспринципные расхитители, не имеющие моральных барьеров и ворующие только потому, что представилась такая возможность. Для подобных «белых воротничков» характерен недолгий срок службы на должности до

начала злоупотреблений. Довольно часто за таким имеется криминальное прошлое.

3. Квазивынужденные расхитители, попавшие в тяжелое материальное положение, в материальную или иную зависимость от лица, требующего совершить хищение или мошенничество. Как правило, подобные проблемы трудно скрыть от окружающих - крупный проигрыш, наркомания, семейный кризис, неудачи в бизнесе. Эта группа расхитителей менее осторожна, они не могут долго подготавливать свои преступления, как это делают первые и вторые.

«Антисоциальный тип» (наименование условное). Также отмечались интернет-мошенники, которые руководствовались не только извлечением прибыли. Более того, их преступный доход часто бывал меньше, чем средняя зарплата специалиста той же квалификации. Мотивом для совершения мошенничества являлась антисоциальная психопатия (социопатия) таких лиц и их патологическая тяга к ведению подобных «игр».

Другие способы совершения преступления.

– Клевета, оскорбления и экстремистские действия в Сети.

– DoS-атаки - способ или атака типа «отказ в обслуживании» является одним из видов неправомерного доступа, а именно такого, который приводит к блокированию информации и нарушению работы ЭВМ и их сети.

– Дефейс - тип хакерской атаки, при которой главная (или другая важная) страница вебсайта заменяется на другую.

– Вредоносные программы

– Кардерство - это мошенническая деятельность с пластиковыми картами с целью извлечения прибыли.

– Нарушение авторских прав в офлайн, нарушение авторских прав в Сети

– Фишинг - это выманивание у потерпевших их конфиденциальных данных методами социальной инженерии

– Киберсквоттинг - этим термином именуется приобретение доменного имени с целью его недобросовестного использования либо с целью не допустить его добросовестного использования другим лицом.

Потерпевший. Очевидно, что потерпевший ранее уже пользовался услугами интернет-магазинов, поскольку само использование этого вида торговли для обычного человека непривычно, требуется время, чтобы решиться и привыкнуть покупать товары таким способом. Столь же очевидно, что потерпевший является пользователем одной из платежных систем, которые использовали мошенники. Также потерпевшему свойственно до последнего момента надеяться, что его все-таки не обманули или это было сделано неумышленно.

Этапы

Криминалистический процесс, который проводят специалисты и эксперты, принято делить на четыре этапа:

1) сбор;

2) исследование;

3) анализ;

4) оформление результатов.

На первом этапе происходит сбор как информации самой по себе, так и носителей компьютерной информации. Сбор должен сопровождаться атрибутированием (пометкой), указанием источников и происхождения данных и объектов. В процессе сбора должны обеспечиваться сохранность и целостность (неизменность) информации, а в некоторых случаях также ее конфиденциальность. При сборе иногда приходится предпринимать специальные меры для фиксации недолговечной информации, например, текущих сетевых соединений или содержимого оперативной памяти компьютера.

На втором этапе производится экспертное исследование собранной информации (объектов носителей). Оно включает извлечение/считывание информации с носителей, декодирование и вычленение из нее той, которая относится к делу. Некоторые исследования могут быть автоматизированы в той или иной степени. Но работать головой и руками на этом этапе эксперту все равно приходится. При этом также должна обеспечиваться целостность информации с исследуемых носителей.

На третьем этапе избранная информация анализируется для получения ответов на вопросы, поставленные перед экспертом или специалистом. При анализе должны использоваться только научные методы, достоверность которых подтверждена.

Четвертый этап включает оформление результатов исследования и анализа в установленной законом и понятной неспециалистам форме.

Оперативно розыскные мероприятия. При раскрытии компьютерных преступлений на вероятность успеха сильно влияет взаимодействие с двумя видами субъектов: специалистами и операторами связи. Настолько

сильной корреляции между содействием с их стороны и успехом раскрытия нет, пожалуй, ни для каких других типов преступлений. Специальные знания в области ИТ, телекоммуникаций, программирования и защиты информации требуются буквально на каждом этапе – от обнаружения признаков преступления до поддержания обвинения в суде. Источником специальных знаний является специалист. Со стороны следователя или оперуполномоченного было бы слишком самонадеянно рассчитывать на собственные знания в этих областях. Настоящим ИТ профессионалом становятся после обучения в вузе и нескольких лет работы по соответствующей специальности. Получить эквивалентные знания, прочитав книги, побеседовав со специалистами и расследовав десяток другой компьютерных преступлений, никак не возможно. Хотя иллюзия всезнания может возникнуть. Ею часто страдают начинающие. Для таких даже существует особый термин дилетант, «чайник», который считает себя знающим. Специфика этой отрасли такова, что в процессе обучения довольно трудно увидеть свой «горизонт незнания», чтобы адекватно оценить собственный уровень.

Особенности осмотра компьютера. Когда следы совершенного преступления и возможные доказательства находятся в цифровой форме (в форме компьютерной информации), их получение, фиксация и документирование представляют определенную сложность. В отличие от многих иных видов доказательств, компьютерная информация не может восприниматься человеком непосредственно – глазами, ушами, пальцами. Воспринимать ее можно только через посредство технических аппаратных и программных средств. Причем количество и сложность этих технических посредников настолько велики, что связь между исходной информацией и тем, что мы видим не экране, не слишком прямая и далеко не всегда очевидная. Следует признать, что осмотр компьютерной информации – это не вполне осмотр, а скорее инструментальная проверка, требующая определенных знаний об используемых технических средствах, принцип действия которых не всегда очевиден. Вероятность ошибиться и увидеть не то, что есть на самом деле, при этом повышенная, даже при отсутствии целенаправленного воздействия противника. Высказывалось мнение, что на основании вышеизложенного осмотр компьютерной информации вообще недопустим, а следует всегда проводить экспертизу.

Особенности тактики обыска. Когда искомые доказательства могут содержаться на компьютерных носителях, обыск следует проводить согласно нижеизложенным правилам, чтобы обеспечить законность и доказательную силу.К компьютерным носителям информации относятся съемные и несъемные магнитные диски, компакт - диски (CD), DVD диски, флэш - накопители, оптические диски, магнитные карты, цифровые кассеты и некоторые другие. Такие носители могут содержаться в персональных компьютерах, серверах, коммуникационном оборудовании, наладонных компьютерах (КПК, PDA), коммуникаторах, смартфонах, мобильных телефонах, цифровых фотоаппаратах и видеокамерах, плеерах и иной другой подобной технике – вся такая техника со встроенными носителями изымается целиком. Другие виды техники не содержат доступных пользователю носителей компьютерной информации, поэтому ее изымать или исследовать не обязательно. Таковыми являются: принтеры, сканеры, факс - аппараты, а также клавиатуры, мониторы, мыши, джойстики, звуковые колонки. Следует помнить, что техника стремительно развивается и доступные пользователю носители могут завтра появиться в составе таких устройств, какие еще сегодня их не имеют.

Особенности работы с потерпевшими. Компьютерная информация имеет свойство легко и быстро утрачиваться. Задержка при сборе доказательств может привести к их неполучению. Поэтому потерпевших и свидетелей надо опросить на предмет таких доказательств как можно быстрее, не дожидаясь официального допроса. *У потерпевших и очевидцев следует узнать следующее.* Преступления, связанные с электронной почтой:

- адреса электронной почты – корреспондента и его собственный;

- сохранилось ли сообщение электронной почты (письмо), где именно оно сохранено;

- если сообщение сохранено, п просите передать его так, чтобы были доступны ВСЕ служебные заголовки, как это сделать, зависит от ис пользуемой программы клиента;

- какая программа клиент использовалась либо какой вебинтерфейс.

Органами внутренних дел РК в текущем году зарегистрированы факты хищений денежных средств с банковских счетов с ис-

пользованием вредоносных программ. Неправомерный доступ осуществлен к информационным системам трех банков второго уровня. «Хакерами использовались вредоносные программы, которые обеспечивали удаленный доступ к управлению денежными средствами», — сообщили в МВД РК. Ранее сообщалось, что хакерским атакам подверглись "Нурбанк" и "Банк ЦентрКредит". В марте 2023 г. Kaspi Bank, Halyk Bank, Qazkom, "Банк Астаны" и "Сбербанк" обратились к казахстанцам. Как отметили банки второго уровня, за последние несколько недель международные кибермошенники предприняли ряд попыток хищения денег с банковских счетов казахстанцев. Однако финансовые институты заверили, что банковские онлайн-сервисы надежно защищены от взлома.

В связи с актуальностью предотвращения преступлений, имеющих цифровые следы, сегодня во всем цивилизованном мире возрастает значение форензики и, следовательно, потребность подготовки специалистов, владеющих теорией и практикой применения знаний о цифровых доказательствах в деятельности следователя, дознавателя криминалиста, эксперта. Форензика, с одной стороны, имеет четко выраженную техническую составляющую, с другой имея приложение к обеспечению судопроизводства доказательствами, непосредственно является частью юридических знаний. Именно такой подход позволит обеспечить криминалистическую подготовку правоохранительных органов расследования к решению обозначенных вопросов на современном уровне.

Список использованных источников:

1. Шухова Н.В., Снигирев А.Л. О роли форензики в криминалистическом обеспечении расследования преступлений. – Новосибирск, ВИ МВД России, 2011.
2. Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.
3. Федотов Н.Н. Форензика – цифровая криминалистика. – М., 2007. С.15.
4. Шухова Н.В. Некоторые информационные аспекты расследования нераскрытых преступлений // Проблемы Информационные технологии в криминалистике – 2008. С.3-5
5. Ярмак К.В.О возможностях использования 3D-технологий в судебной экспертизе. -Московский университет МВД России, 2010.

References:

1. Shukhova N.V., Snigirev A.L. O roli forenziki v kriminalisticheskom obespechenii rassledovaniya prestupleny. – Novosibirsk, VI MVD Rossii, 2011.
2. Fedotov N.N. Forenzika – kompyuternaya kriminalistika – M.: Yuridichesky Mir, 2007. – 432 s.
3. Fedotov N.N. Forenzika – tsifrovaya kriminalistika. – M., 2007. S.15.
4. Shukhova N.V. Nekotorye informatsionnye aspekty rassledovaniya neraskrytykh prestupleny // Problemy Informatsionnye tekhnologii v kriminalistike – 2008. S.3-5
5. Yarmak K.V.O vozmozhnostyakh ispolzovaniya 3D-tekhnology v sudebnoy ekspertize. -Moskovsky universitet MVD Rossii, 2010.