

УДК: 343. 451

Владимир Голубев
к.ю.н., профессор кафедры уголовного права и правосудия
юридического факультета ЗНУ

Некоторые вопросы расследования компьютерных преступлений

Расследование компьютерных преступлений существенно отличаются от расследований других "традиционных" преступлений. По данным уголовным делам чаще всего допускаются ошибки, что, зачастую объясняется отсутствием надлежащего уровня теоретической и практической подготовки оперативных работников и следователей. Изучение уголовных дел этой категории дает основание полагать, что одной из существенных причин низкого качества следствия является отсутствие систематизированных и отработанных методов расследования компьютерных преступлений, а также ошибки, которые совершаются при проведении следственных действий в отношении компьютерной информации либо самих компьютеров.

Результаты анализа практической деятельности правоохранительных органов по расследованию компьютерных преступлений свидетельствуют о том, что исследование компьютерной техники целесообразно проводить в условиях криминалистической лаборатории, где эту работу выполняют специалисты с необходимой профессиональной подготовкой.

Доказательства, связанные с компьютерными преступлениями и изъяты с места происшествия, могут быть легко изменены, как в результате ошибок при их изъятии, так и в процессе самого исследования. Представление подобных доказательств в судебном процессе требует специальных знаний и соответствующей подготовки. Здесь нельзя недооценивать роль экспертизы, которая может дать квалифицированный ответ на поставленные вопросы.

Однако экспертиза требует какого-то времени не только на ее проведение, но и на поиск соответствующих специалистов, а при изъятии компьютерной техники существенным фактором, позволяющим сохранить необходимую доказательную информацию, является неожиданность и оперативность. Именно поэтому изъятие компьютеров и информации приходится проводить теми силами, которые в настоящее время проводят следственные действия. В данном случае именно следователь не застрахован от ошибок, обусловленных недостаточностью знаний, что потом достаточно умело, используется защитой в суде.

Поставленная проблема имеет два аспекта: общие ошибки, которые допускаются работниками правоохранительных органов при расследовании компьютерных преступлений, и технические аспекты,

связанные с защитой информации, которая устанавливается на компьютерах их непосредственными пользователями.

Как известно, обнаружение, осмотр и изъятие компьютеров и компьютерной информации в процессе следственных действий могут совершаться не только при следственном осмотре (ст. 190 КПК), но и при проведении других следственных действий: обыски (ст. 178 КПК); выемки (ст. 179 КПК); воспроизведения обстоятельств и обстановки происшествия (ст. 194 КПК).

Следует выделить некоторые правила работы с компьютерами, изъятиями при расследовании преступлений в сфере компьютерной информации, а также предложить общие рекомендации, которые могут быть полезными при обработке компьютерных доказательств.

Рассмотрим некоторые типичные ошибки, наиболее часто совершаемые при проведении следственных действий в отношении компьютерной информации либо самих компьютеров.

Ошибка - 1.

Ошибочная работа с компьютером

Первое и основное правило, которое должно неуклонно выполняться, состоит в следующем: никогда и ни при каких условиях не работать на изъятом компьютере. Это правило допускает, что изъятый компьютер - прежде всего объект исследования специалиста. Поэтому до передачи экспертам его желательно даже не включать, поскольку категорически запрещено исполнять любые операции на изъятом компьютере, не обеспечив необходимых мер защиты (например, защиты от модификации или создания резервной копии). Если на компьютере установлена система защиты (например - пароль), то его включение может вызвать уничтожение информации, которая находится на жестком диске. Не допускается загрузка такого компьютера с использованием его собственной операционной системы.

Подобная мера объясняется достаточно просто: преступнику не составляет особого труда установить на своем компьютере программу для уничтожения информации на жестком или гибком магнитном диске, записав также "ловушки" через модификацию операционной системы. Например, простая команда DIR, которая используется для отображения каталога диска, может быть легко изменена, чтобы отформатировать жесткий диск.

После того, как данные и сама разрушительная программа уничтожены, никто не сможет сказать наверняка, был ли "подозреваемый" компьютер оборудован такими программами специально, или это результат небрежности при исследовании компьютерных доказательств?

Ошибка - 2.

Допуск к компьютеру владельца (пользователя) компьютера

Серьезной ошибкой является допуск к исследуемому компьютеру владельца для оказания помощи в его эксплуатации. Известны многие случаи из практики, когда подозреваемые на допросах, связанных с компьютерными доказательствами, допускались к работе на изъятом компьютере. Позже они рассказывали своим знакомым, как шифровали файлы "прямо под носом у полицейских", а те об этом даже не догадывались. Учитывая такие последствия, компьютерные специалисты стали делать резервные копии компьютерной информации прежде, чем допускать к работе над ней.

Еще одна проблема связана с возможностью опровержения в суде идентичности предъявленного на процессе программного обеспечения тому, которое находилось на данном компьютере на момент изъятия. Чтобы избежать подобных ситуаций, компьютер, следует опечатать в присутствии понятых, не включая. Если работник правоохранительных органов принимает решение об осмотре компьютера на месте, первое, что необходимо сделать, это снять копию с жесткого магнитного диска и любой дискеты, которая будет изыматься как вещественное доказательство. Это означает, что до проведения каких-либо операций с компьютером, необходимо зафиксировать его состояние на момент проведения следственных действий.

Ошибка-3.

Отсутствие проверки компьютера на наличие вирусов и программных закладок.

С целью проверки компьютера на наличие вирусов и программных закладок, необходимо загрузить компьютер не с его операционной системы, а со своей загодя подготовленной дискеты, либо со стандового жесткого диска. Проверке подвергаются все носители информации - дискеты, жесткий диск и другие носители. Эту работу следует сделать привлеченному к участию в следственных действиях специалисту с помощью специального программного обеспечения.

Нельзя допустить, чтобы у суда появилась возможность обвинения следствия в умаленном заражении компьютера вирусами, в некомпетентности при проведении следственных действий, либо просто в небрежности, поскольку доказать, что вирус находится в компьютере до момента исследования, вряд ли возможно, а подобное обвинение поставит под сомнение всю работу эксперта и достоверность его выводов.

Такие наиболее типичные ошибки, которые часто встречаются при исследовании компьютера в делах, связанных с расследованием компьютерных преступлений. Однако рассмотренный перечень не охватывает всех ошибок, возникающих в процессе изъятия и исследования компьютерной информации. Этому можно легко дать объяснение: отсутствие достаточного опыта в подобных делах в нашей стране. В то же время в странах Западной Европы и США уже накоплен богатый опыт расследования сложных компьютерных преступлений. Необходимо более тщательно его изучить, что позволит избежать многих из них.

Во избежание ошибок при проведении следственных действий на начальном этапе расследования, которые могут привести к потере или искажению компьютерной информации, следует придерживаться некоторых предохранительных мер.

Рекомендация - 1.

В первую очередь следует сделать резервную копию информации.

В процессе обыска и изъятия, связанных с изъятием компьютера, магнитных носителей и информации, возникает ряд общих проблем, связанных со специфичной изымаемых технических средств.

В первую очередь необходимо предусмотреть меры безопасности, которые совершаются преступниками с целью уничтожения компьютерной информации. Они, например, могут использовать специальное оборудование, в критических случаях образующее спящее магнитное поле, которое стирает магнитные записи.

На протяжении обыска все электронные доказательства, находящиеся в компьютере либо в компьютерной системе должны быть собраны таким образом, дабы они потом могли быть признаны судом. Мировая практика показывает, что в большинстве случаев под давлением представителей защиты в суде электронные доказательства не принимаются во внимание. Чтобы гарантировать их признание в качестве доказательств, необходимо строго придерживаться уголовно-процессуального законодательства, а также стандартизированных приемов и методов их изъятия.

Обычно компьютерные доказательства скрываются путем создания точной копии с оригинала (первичного доказательства), прежде чем делается какой-либо их анализ. Но делать копии компьютерных файлов, используя только стандартные программы резервного копирования, недостаточно. Вещественные доказательства могут существовать в виде уничтоженных либо спрятанных файлов, а данные, связанные с этими файлами, можно скрывать только с помощью специального программного обеспечения. В самом простом виде это могут быть программы типа - SafeBack, а для гибких дисков бывает достаточно программы DOS Discopy.

Магнітні носії, на які передбачається копіювати інформацію, повинні бути заздалегідь підготовлені (необхідно переконатися, що на них немає жодної інформації). Носії слід зберігати в спеціальних упаковках або заворачивать в чисту папір. Необхідно пам'ятати, що інформація може бути пошкоджена вологістю, температурним впливом або електростатичними (магнітними) полями.

Рекомендація - 2.

Найти и сделать копии временных файлов.

Многие текстовые редакторы и программы управления базами данных создают временные файлы как побочный продукт нормальной работы программного обеспечения. Большинство пользователей компьютера не осознают важности создания этих файлов, потому что обычно они уничтожаются программой в конце сеанса работы. Однако данные, находящиеся внутри этих уничтоженных файлов, могут оказаться наиболее полезными. Особенно, если исходный файл был кодированный или документ подготовки текстов был напечатан, но никогда не сохранялся на диске, такие файлы могут быть восстановлены.

Рекомендація - 3.

Необходимо обязательно проверить Swap File.

Популярность Microsoft Windows принесла некоторые дополнительные средства, касающиеся исследования компьютерной информации. Swap File функционируют как дисковая память, огромная база данных и множество разных временных фрагментов информации. В этом Swap File может быть обнаружен даже весь текст документа.

Рекомендація - 4.

Необходимо сравнивать дубли текстовых документов.

Часто дубли текстовых файлов можно обнаружить на жестком либо гибком магнитных дисках. Это могут быть незначительные изменения между версиями одного документа, которые могут иметь доказательную ценность. Расхождения можно легко идентифицировать с помощью наиболее современных текстовых редакторов.

Хотелось бы выделить также общие рекомендации, которые необходимо учитывать при исследовании компьютера на месте происшествия.

Приступая к осмотру компьютера, следователь и специалист непосредственно производящий все действия на ЭВМ, должны придерживаться следующего:

- перед выключением компьютера необходимо по возможности закрыть все используемые на компьютере программы. Следует помнить о том, что некорректный выход с некоторых программ может вызвать уничтожение информации или испортить саму программу;
- принять меры по установлению пароля доступа к защищенным программам;
- при активном вмешательстве сотрудников предприятия, стремящихся противодействовать следственной группе,

необходимо отключить электропитание всех компьютеров на объекте, опечатать их и изъять вместе с магнитными носителями для исследования информации в лабораторных условиях;

· в случае необходимости консультаций персонала предприятия, получать их следует у разных лиц путем опрашивания или допроса. Подобный метод позволит получить максимально правдивую информацию и избежать умышленного вреда;

· при изъятии технических средств, целесообразно изымать не только системные блоки, но и дополнительные периферийные устройства (принтеры, стримеры, модемы, сканеры и т.п.);

· при наличии локальной вычислительной сети необходимо иметь нужное количество специалистов для дополнительного исследования информационной сети;

· изымать все компьютеры (системные блоки) и магнитные носители;

· тщательно осмотреть документацию, обращая внимание на рабочие записи операторов ЭВМ, ибо часто именно в этих записях неопытных пользователей можно обнаружить коды, пароли и другую полезную информацию;

· составить список всех внешних и временных работников организации (предприятия) с целью выявления программистов и других специалистов в области информационных технологий, работающих в данном учреждении. Желательно установить их паспортные данные, адреса и места постоянной работы;

· записать данные всех лиц, находящихся в помещении на момент появления следственной группы, независимо от объяснения причин их пребывания в данном помещении;

· составить список всех сотрудников предприятия, имеющих доступ к компьютерной технике либо часто пребывающих в помещении, где находятся ЭВМ.

Если возможен непосредственный доступ к компьютеру и исключены все нежелательные ситуации, приступают к осмотру. При этом следователь и специалист должны четко объяснить все свои действия понятным.

При осмотре должны быть установлены:

- конфигурация компьютера с четким и подробным описанием всех устройств;
- номера моделей и серийные номера каждого из устройств;
- инвентарные номера, присваиваемые бухгалтерией при постановке оборудования на баланс предприятия;
- другая информация с фабричных ярлыков (на клавиатуре ярлык обычно находится на обратной стороне, а на мониторе и процессоре - сзади). Такая информация вносится в протокол осмотра вычислительной техники и может быть важной для следствия.

Рекомендація - 5

Фотографування і маркування елементів комп'ютерної системи.

Фотографування і маркування елементів комп'ютерної системи - важкий перший шаг при підготовці системи к транспортуванню. Документування стану системи на даному етапі необхідно для правильної зборки і підключення всіх елементів системи в умовних лабораторних. При фотографуванні слід виконати знімки системи крупним планом її передньої і задньої частини. Фотографування і маркування елементів вивілкової комп'ютерної системи дає можливість в точності воссоздати стану комп'ютерної техніки в лабораторних умовних дослідження. Некекторе оборуванне типу зовнішніх модемів може мати мнжество мелких переключачей, фіксуруючих его стану, котрі при транспортуванні можуть бути

змненені, що створить додаточні проблеми для експерта.

В заклоченні необхідно підчеркнути, що при проведенні любых следственних дійствий, звязаних с расследованием преступлений в сфере использования компьютерных технологий (особенно вилемка информации и компьютерного оборування) целесообразно с самого начала привлечение специалиста в области информационных технологий. До начала следственных действий следует также иметь определенную информацию, касающуюся: марки, модели, компьютера, операционной системы, периферийных устройств, средств связи и любых других ведомостей о системе, которая является объектом расследования. Целенаправленная деятельность следователя, оперативных работников, особенно на первичном этапе расследования, обеспечивает успех дальнейшего расследования компьютерных преступлений.

УДК: 343. 713: 343. 8 (477)

Дьоменко С.В.

Ст. викладач кафедри кримінального права та правосуддя юридичного факультету ЗНУ

Деякі теоретичні та практичні проблеми запобігання вимагань

Протидія злочинності - один з важливих напрямків розбудови України як незалежної демократичної держави. Ця діяльність значною мірою залежить від теоретичних розробок протидії окремим видам злочинності.

Одним з небезпечних злочинів проти власності є вимагання. Його суспільна небезпека полягає не тільки у посяганні на майно або майнові права, а у застосуванні при цьому погроз різного характеру, а іноді й насильства в тому числі й такого, яке є небезпечним для життя чи здоров'я особи, знищуванні майна потерпілого та його близьких родичів тощо.

Враховуючи суспільну небезпеку цього виду злочину, актуальною є активна цілеспрямована протидія вимаганню. Слід зазначити, що за часів існування колишнього Радянського Союзу вимагання вивчалися багатьма вченими і в першу чергу тими, хто досліджував злочини проти власності. У зв'язку з цим, можна назвати прізвища таких вчених як В.І. Анципов, Г.М. Борзенкова, В.О. Владимиров, А.І. Волобуєва, Є.Б. Галкіна, М.А. Гельфер, О.І. Гурова, О.В. Дмитрієва, В.П. Ємельянов, В.А. Клименко, В.М. Куц, Ю.І. Ляпунов, В.І. Литвинков, П.С. Матишевський, М.І. Мельник, В.С. Мінськой, В.С. Нікіфоров, В.М. Сафонова, С.І. Тихенко та ін.

Слід особливо підкреслити ґрунтовність дисертаційної роботи М.І. Мельника, присвяченої

кримінально-правовим аспектам цього виду злочинів. Кримінологічний аспект вимагань в Україні взагалі не досліджувався, навіть ця тема не виділялась у підручниках з кримінології. Отже, актуальною є розробка кримінологічного аспекту вимагань, зокрема діяльності із запобігання цих злочинів.

В українській кримінологічній літературі до цього часу не сформувався єдине розуміння поняття запобігання злочинності. У підручниках з кримінології і в наукових роботах застосовуються як поняття попередження злочинності, окремих її видів і конкретних злочинів, так і поняття профілактика, запобігання. При цьому, одна група авторів отожднює ці поняття, а інша - вкладає в них різний зміст. Так, наприклад, В.В. Голіна окремо виділяє термін попередження, як більш широкое поняття, що охоплює профілактику, запобігання, припинення злочинних проявів. Кожен з цих термінів, на думку автора, має свій зміст, свій специфічний напрям діяльності [1].

Вважаємо більш прийнятною є точка зору тих авторів, які отожднюють вказані поняття. У зв'язку з цим, Я.Ю. Кондратьєв та О.М. Джужа зазначають, що "...розрізнення цих понять є надуманим, таким, що суперечить буквальному змісту вказаних слів. Кожен з них означає одне й те саме: упередити, не допустити. Усі ці слова є взаємозамінними синонімами. Тому заходи рівнозначно можуть бути або попереджувальні, або профілактичні, або запобіжні, або превентивні.