



*Владимир Губеев  
кандидат юридических наук,  
профессор кафедры уголовного права и правосудия ЗГУ*

## **Криминалистическая характеристика незаконного вмешательства в работу электронно-вычислительных машин**

Актуальность темы статьи обусловлена тем, что современная следственная практика и успех расследования любого преступления зависит не только от способности следователя выявлять и оценивать входящие в предмет доказывания фактические данные, но и в значительной степени от его умения проникать в криминалистическую суть расследуемой преступной деятельности. Существенную помощь в выявлении, раскрытии и расследовании преступлений в сфере использования электронно-вычислительных машин (ЭВМ) может оказать детальная проработка криминалистической характеристики преступлений данного вида. При этом крайне важно точно понимать смысл норм материального права, описывающих предмет доказывания и определяющих цели процесса расследования.

Целью этой статьи стало исследование совокупности наиболее характерных криминалистически значимой взаимосвязанной информацией о признаках и особенностях незаконного вмешательства в работу ЭВМ. Исходя из этой цели задачами исследования стали: определение и формирование криминалистической характеристики незаконного вмешательства в работу ЭВМ (на основе данных о способах совершения, сокрытия, обстановке, орудиях и средствах совершения преступления, следах, механизме противоправного посягательства, а также личностных свойствах граждан, осуществивших незаконное вмешательство в работу ЭВМ).

Учитывая новизну решений законодателя в области признания уголовно наказуемыми деяний, касающихся преступлений в сфере использования электронно-вычислительных машин, любое исследование криминальной деятельности следует начинать с определения сущности новых понятий, введенных законодателем при конструировании состава преступления.

Анализ раздела XVI Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей Уголовного кодекса Украины (УК) показывает, что законодатель ввел ряд понятий, не содержащихся ранее не только в уголовно-правовой терминологии, но и в законодательстве, регулирующем информационные отношения. Эти термины нуждаются в существенных пояснениях, основанных на понимании как ряда технических характеристик новых средств обработки информации, так и сущности самой информации как новой уголовно-правовой и криминалистически значимой категории.

Учитывая важность определения смыслового значения термина "незаконное вмешательство", в общем,

не характерного для традиционных уголовно-правовых описаний способа действия, рассмотрим это понятие с точки зрения действующего законодательства.

Анализ ст. 361 УК показывает, что поднезаконным вмешательством в работу ЭВМ, их систем или компьютерных сетей, законодатель подразумевает проникновение в эти машины, их системы или сети и совершение действий, которые изменяют режим работы машины, ее системы или компьютерной сети, или же полностью или частично прекращают их работу, без разрешения (согласия) соответствующего собственника или уполномоченного ним лица, а также влияют на работу ЭВМ с помощью разных технических устройств, способных повредить работе машины.

Ст. 361 УК защищает право собственника на неприкосновенность информации в автоматизированных электронно-вычислительных машинах, их системах или компьютерных сетях. Собственником информационной автоматизированной системы может быть любое лицо, которое правомерно пользуется услугами обработки информации как собственник такой системы (ЭВМ, их систем или компьютерных сетей) или как лицо, имеющее право пользования такой системой.

Преступное действие, ответственность за которое предусмотрена в ст. 361 УК, должно состоять из незаконного вмешательства в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей, что всегда имеет характер совершения определенных действий, и может выразиться в проникновении в компьютерную систему путем использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты с незаконного применения установленных паролей или маскировки под видом законного пользователя с целью проникновения в компьютерную систему.

Так, ч.1 ст. 361 УК в качестве уголовно-наказуемого действия закрепляет "незаконное вмешательство в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей, что привело к искажению или уничтожению компьютерной информации или носителей такой информации". Этот состав преступления материальный. Последствия являются обязательным элементом его объективной стороны. Однако закон содержит ограниченный перечень вредных последствий в разных формах, кроме прямо указанных в ст. 361 УК.

Лицо, совершившее указанные действия в формах, не указанных в ст. 361 УК, уголовной ответственности не подлежит.

Н.Н. Ахтарская, П.Д. Вепенчук, В.Б. Везов, А.Г. Волков, Ю.В. Гавришин, Н.В. Гудалюк, В.Е. Козлов, В.В. Крылов, В.А. Минаев, Н.А. Розенфельд, Е.Р. Россиновская, Н.В. Салгевский, О.П. Ситтерев, В.С. Цимбалюк, В.М. Червасов, Н.Г. Шурузов и др. - вот далеко не полный список ученых, которые на протяжении 1996-2004 г. исследовали проблемы противодействия и борьбы с преступлениями в сфере использования ЭВМ.

Однако в их работах, не рассматривались вопросы расследования незаконного вмешательства в работу электронно-вычислительных машин как отдельного преступления. В то же время, сотрудники органов внутренних дел и других правоохранительных органов, занимающиеся расследованием данного вида преступлений, испытывают потребность в научно-обоснованной методике расследования. В целях научного осмысления проблемы необходимо разработать криминалистическую характеристику данного преступления.

Теоретические положения обобщенной криминалистической характеристики преступлений были разработаны П.С. Белкиным, А.Н. Васильевым, В.А. Образцовым, В.Ю. Шелестово, Н.П. Яблочкиным и др.

Представляет интерес суждения В.П. Корж, которая исследуя понятие и структуру криминалистической характеристики эвонимических преступлений, совершаемых организованными преступными группами (ОПГ) выделяет их особенности, специфику, признаки, обстановку совершения преступления, следы и иные последствия указанных преступлений [1].

Н.Г. Шурузов определяет криминалистическую характеристику преступления как отражение системы криминалистических черт, свойств, признаков преступления, отображающихся в объективной действительности. Она, отмечает далее он, содержит данные о типичных способах совершения и сокрытия преступления, механизме преступного посягательства, следах, обстановке, в которой готовилось и произошло преступное событие, предпосылках преступного посягательства, чертах личности преступника и потерпевшего, а так же обстоятельствах, способствующих совершению преступления [2].

По мнению В.Б. Везова в структуру криминалистической характеристики необходимо включать криминалистически значимые сведения о личности правонарушителя, мотивации и цели его преступного поведения, а также сведения о потерпевшей стороне [3].

Заслуживает серьезного внимания точка зрения В.Е. Козлова. Он под криминалистической характеристикой компьютерных преступлений понимает наиболее характерную, криминалистически значимую взаимосвязанную информацию о признаках и свойствах такого рода преступлений, способную служить основанием для выдвижения версий о событии преступления и личности преступника [4].

Большинство отечественных и зарубежных ученых едины в том, что криминалистическая характеристика является важным элементом структуры криминалистической методики расследования преступлений в сфере использования ЭВМ.

Под криминалистической методикой раскрытия и расследования преступлений в сфере использования ЭВМ следует понимать совокупность научных положений и рекомендаций, разработанных на основе до сих пор научно обоснованных и апробированных на практике наставлений по раскрытию и расследованию данных преступлений.

Сравнивая различные определения криминалистической характеристики, можно сделать вывод, что большинство исследователей-криминалистов отмечают следующие элементы криминалистической характеристики: типичные следственные ситуации; способы совершения преступления; типичные

материальные следы преступления; характеристика личности обвиняемого и потерпевшего; способ сокрытия преступления; обстановка преступления.

Указанный подход позволяет выделить ряд проблемных вопросов в процессе формирования криминалистической характеристики незаконного вмешательства в работу ЭВМ:

- выходя личность преступлений в сфере использования электронно-вычислительных машин. Так В.С. Цимбалюк отмечает, что основной ее причиной является то, что в большинстве случаев, из-за нежелания подрыва репутации, потерпевшие неохотно сообщают правоохранительным органам о фактах преступных посягательства на их компьютерные системы [5];
- сложность сбора доказательств и процесса доказывания в суде;
- достаточно широкий спектр криминалистически значимых признаков в компьютерных преступлениях;
- отсутствие четкой программы борьбы с компьютерными преступлениями;
- сложность самого процесса раскрытия (в узком понимании слова) компьютерных преступлений;
- отсутствие достаточной следственной практики по расследованию компьютерных преступлений.

Под криминалистической характеристикой незаконного вмешательства в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей мы понимаем систему обобщенных данных о типичных следах, способах совершения и механизмах преступления, личности преступника и других существенных чертах, свойствах и особенностях преступления и способствующих ему обстоятельствах, что помогает оптимизации расследования и правящего ему применению средств, приемов и методов криминалистики в раскрытии и расследовании данного преступления. Ее составляют следующие основные данные о: способах совершения преступления и механизме противоправного действия; способах сокрытия незаконного вмешательства в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей; орудиях (средствах) совершения противоправного деяния; обстоятельствах и месте совершения преступления; следах преступления; предметах преступного посягательства; лицах, совершивших незаконное вмешательство в работу ЭВМ (компьютеров), систем и компьютерных сетей и т.д.

Рассмотрим данные о способах совершения преступления и механизме противоправного деяния. Под способом преступления понимается система объединенных единым замыслом действий преступника (и связанных с ними лиц) по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами и сопряженных с использованием соответствующих орудий и средств. На сегодняшний день нет четкой классификации способов совершения незаконного вмешательства в работу ЭВМ, однако большинство способов совершения незаконного доступа к ЭВМ можно объединить в три основные группы.

Первая группа - это способы непосредственного доступа. При их реализации информация уничтожается, блокируется, модифицируется, копируется, а так же может нарушаться работа ЭВМ, системы ЭВМ или их сети путем отдачи соответствующих команд с компьютера, на котором информация находится. Непосредственный доступ может осуществляться как лицами, работающими с информацией (имеющими отношение к этой работе), так и лицами, специально проникшими в закрытые зоны и помещения, где производится обработка информации. Это может осуществляться, например, следующим образом: лицо, имеющий умысел на незаконный доступ к ЭВМ, держа в руках определенные предметы, указывающие на его "принадлежность" к работе на компьютере (дискеты, распечатки и пр.) проламывается около закрытой двери помещения, где расположены ЭВМ.

Дождавшись, когда в названное помещение входит работающий в нем сотрудник, входит туда вслед за ним, а затем совершает незаконный доступ к ЭВМ.

Вторая группа включает способы опосредованного (удаленного) доступа к компьютерной информации.

При этом неправомерный доступ к определенному компьютеру и находящаяся на нем информация осуществляется с другого компьютера, находящегося на определенном расстоянии, через компьютерные сети. К способам опосредованного (удаленного) доступа можно отнести:

1. Подключение к линии связи законного пользователя (например, к телефонной линии) и получение тем самым доступа к его системе и ЭВМ.

2. Проникновение в чужие информационные сети, путем автоматического перебора абонентских номеров с последующим соединением с тем или иным компьютером (перебор осуществляется до тех пор, пока на другом конце линии не "позвонит чужой" компьютер).

3. Незаконный доступ к ЭВМ с использованием чужих паролей, выдавая при этом себя за законного пользователя. При подобном способе незаконный пользователь осуществляет подбор пароля для доступа к чужому компьютеру. Для реализации такого подбора существуют уже специально разработанные программы, которые легко могут быть найдены и "скачены" с многочисленных хакерских сайтов в Интернет. Подобранный индивидуальный пароль незаконный пользователь получает доступ к ЭВМ и может проводить с ней любые действия под видом законного пользователя: копировать или модифицировать информацию, удалять или запускать программы, производить операции, например, по переводу денежных средств с банковских счетов на свой счет, фальсифицировать платежные документы.

Одним из распространенных орудий незаконного доступа к ЭВМ является сам компьютер. Другим распространенным средством совершения неправомерного доступа в последнее время стала глобальная сеть Интернет.

В августе в Лондоне были арестованы два гражданина Казахстана - Олег Зезов и Игорь Ярмаза - по обвинению во взломе, незаконном проникновении в компьютерную систему известной американской службы финансовых новостей "Bloomberg", а также попытке вымогательства 200 000 долларов у ее основателя и главы - Майкла Блумберга. О. Зезов работал в алмазниковой компании Kazkommerts Securities, которая пользовалась услугами Open Bloomberg, информационной базы данных американской службы новостей.

Воспользовавшись своим клиентским доступом в компьютерную систему Bloomberg, Зезов проник в служебные базы данных компании и получил в свое распоряжение не только логинный пароль доступа самого Блумберга и реквизиты его кредитных карт, пароли администраторов системы, но и конфиденциальные данные 90 000 пользователей информационных терминалов сети Bloomberg. После чего Зезов с помощью электронной почты связался с Майклом Блумбергом и представил ему все доказательства компрометации защиты и потребовал от него 200 000 долларов в обмен на информацию о "даре" в компьютерной системе компании. В противном случае Зезов пригрозил предать истории самую широкую огласку. Только совместной операцией казахских спецслужб и США эти противоправные действия были пресечены, а Олег Зезов со своим подельником арестованы и этапированы в США.

Незаконный доступ к ЭВМ может быть связан и с насилием над личностью либо угрозой его применения. Представляется, что насилие над личностью или угроза его применения могут иметь место при непосредственном, опосредованном и при смешанном способах совершения рассматриваемого преступления. Незаконный доступ к ЭВМ, сопряженный с насилием над личностью или угрозой его применения, может иметь место в том случае, когда незаконный пользователь после применения насилия или под его угрозой, вынужден осуществлять незаконный доступ к ЭВМ.

При этом он производит уничтожение, копирование, модификацию или блокирование информации непосредственно

на том компьютере, где данная информация хранится.

Подобным образом могут осуществляться и смешанные способы незаконного доступа к ЭВМ. К примеру, когда осуществляется физическое воздействие (или его угроза) на программистов (операторов) с целью тайного введения в программу ЭВМ незапланированных команд или ее модификация, применяется насилие для получения слабых мест в системе защиты программной или вычислительной среды (системы ЭВМ или сети), а также разного рода ошибок в логике построения программы и целых их дальнейшее противоправное использование.

Данный о способе сокрытия неправомерного доступа к компьютерной информации. Под сокрытием преступления понимается деятельность (элемент преступной деятельности), направленная на воспрепятствование расследованию путем уничтожения, уничтожения, маскировки или фальсификации следов преступления и преступника и их носителей [6].

Способы сокрытия не законного доступа к ЭВМ в определенной мере детерминированы способами его совершения. В случае непосредственного доступа к ЭВМ сокрытие следов преступления сводится к возмощиванию обстановки, предшествующей совершению преступления, то есть, уничтожение оставленных следов (пальцы в руке, обуги, микрочастицы и т.д.). При опосредованном (удаленном) доступе сокрытие заключается именно в способе совершения преступления, который затрудняет обнаружение незаконного доступа. Это достигается употреблением чужих паролей, средств разграничения доступа и т.д.

Орудиями незаконного вмешательства в работу ЭВМ (компьютеров), систем и компьютерных сетей являются средства компьютерной техники и специальное программное обеспечение. Следует различать средства непосредственного и удаленного доступа.

К средствам непосредственного доступа можно отнести, прежде всего, машинные носители информации, а также все средства преодоления защиты информации. Прием, каждой категории средств защиты (организационно-технические, программно-технические) соответствует свой набор орудий незаконного вмешательства в работу ЭВМ. К орудиям удаленного доступа относятся прежде всего сетевое оборудование (при не санкционированном доступе из локальных сетей), а так же средства доступа в удаленные сети (средства телефонной связи, модем).

Для анализа и расследования незаконного доступа к ЭВМ, имеют данные об обстановке и месте совершения преступления, т.е. все окружающие субъекта условия, в которых осуществляются такие противоправные действия.

Обстановку совершения незаконного доступа к ЭВМ, на наш взгляд составляет вещественные, технические, пространственные, временные, социально-психологические обстоятельства совершения рассматриваемого преступления. Особенностью данного преступления, как впрочем, и других компьютерных преступлений является то, что на него практически не оказывают влияние природно-климатические факторы.

Дополнительными факторами, характеризующими обстановку совершения неправомерного доступа к компьютерной информации могут являться наличие и состояние средств защиты компьютерной техники (организационных, технических, программных), сложившаяся на объекте дисциплина, требовательность со стороны руководителей по соблюдению норм и правил информационной безопасности и эксплуатации ЭВМ и т.п.

Для обстановки, в которой возможно совершение рассматриваемого преступления наиболее свойственно следующее: некая окрестность технико-организационный уровень хозяйственной деятельности, низкий контроль за информационной безопасностью, ненадежная система защиты информации, атмосфера безразличия к случаям нарушения требований информационной безопасности и др.

Выявление особенностей сложившейся обстановки позволяет быстрее определить, на что следует обратить особое внимание при осмотре места происшествия, изучении компьютерного оборудования и документов, вызове и допросе конкретных свидетелей и решении вопросов о необходимости изъятия определенных документов и т.п.

Особенностью незаконного доступа к ЭВМ является то, что место непосредственного совершения противоправного деяния (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат противоправного деяния) могут не совпадать. Прием, это имеет место практически при каждом случае удаленного доступа к ЭВМ. При непосредственном же доступе место совершения противоправного деяния и место наступления вредных последствий совпадают. Также преступления часто совершают сами работники предприятия или организации, учреждения или фирмы. В этой связи можно говорить о том, что компьютерная преступность может иметь транснациональный (трансграничный) характер - преступления совершается в одной юрисдикции, а негативные последствия наступают в другой. Необходимо отметить, что преступления в сфере использования компьютерных технологий все более приобретают транснациональный, организованный и групповой характер. Транснациональный характер компьютерной преступности на сегодняшний день составляет определенную общественную опасность, реально угрожающую национальной безопасности - составляющей национальной безопасности государства.

Данные о следах незаконного доступа к ЭВМ являются важнейшими из элементов криминалистической характеристики преступления. Под следами преступления понимаются любые изменения среды, возникшие в результате совершения в этой среде преступления [7].

Особенность следов, оставшихся при незаконном доступе к ЭВМ является то, что они, в основном, не рассматриваются современной трасологией, поскольку в большинстве случаев, носят информационный характер, то есть представляют собой те или иные изменения в компьютерной информации, имеющие форму ее уничтожения, модификации, копирования, блокирования.

Таким образом, следы незаконного доступа к ЭВМ представляются целесобразным разделить на два типа: традиционные следы (следы-отображения, рассматриваемые трасологией, а так же следы вещества и следы-предметы) и нетрадиционные - информационные следы.

К первому типу относятся материальные следы. Они могут являться какие-либо рукописные записи, распечатки и т.п., свидетельствующие о приготовлении и совершении преступления. Материальные следы могут остаться и на самой вычислительной технике (следы пальцев рук, микрочастицы на клавиатуре, дисководы, принтере и т.д.), а так же на магнитных носителях и CD-ROM дисках.

Информационные следы образуются в результате воздействия (уничтожения, модификации, копирования, блокирования) на компьютерную информацию путем доступа к ней и представляют собой любые изменения компьютерной информации, связанные с событием преступления. Прежде всего, они остаются на магнитных носителях информации и отражают изменения в хранившейся в ней информации (по сравнению с исходным состоянием).

Информационными следами являются так же результаты работы антивирусных и тестовых программ. Данные следы могут быть выявлены при изучении компьютерного оборудования, рабочих записей программистов, протоколов работы антивирусных программ, а так же программного обеспечения. Для выявления подобных следов необходимо участие специалистов.

Информационные следы могут оставаться и при опосредованном (удаленном) доступе через компьютерные сети, например, через "Internet". Они возникают в силу того, что система, через которую производится доступ, обладает некоторой информацией, которую она запрашивает у лица, пытающегося соединиться с другим компьютером. Система определяет электронный адрес, используемое программное обеспечение и его версия. Кроме того, при доступе в сеть обычно запрашивается адрес электронной почты, реальное имя и другие данные. Эту информацию запрашивает системный администратор (провайдер) для контроля обращений на его сервер и это так же позволяет идентифицировать личность лица, проникнувшего в сеть.

Следами, указывающими на незаконный доступ к ЭВМ, могут являться: переименование каталогов и файлов; изменение размеров и содержания файлов; изменение стандартных реквизитов файлов, даты и времени их создания; появление новых каталогов, файлов и т.п.

При незаконном доступе к ЭВМ предметом преступного посяательства является:

- ЭВМ;
- компьютерные системы;
- компьютерные сети.

При незаконном доступе к ЭВМ предметом преступного посяательства является также и компьютерная информация. Несмотря на то, что компьютерную информацию тяжело безоговорочно признать предметом преступления, поскольку она не является вещью материального мира, автор разделяет мнение тех исследователей, которые считают целесообразным несколько расширить общетеоретические понятия предмета преступления. Предлагаю включить в него не только вещи материального мира, но и определенные, объективно существующие явления, образования - компьютерную информацию [8]. Компьютерная информация - это текстовая, графическая или любая другая информация (данные), которая существует в электронном виде, сохраняется на соответствующих носителях и которые можно создавать, изменять или использовать с помощью АЭВМ. Компьютерную информацию так же можно определить и как информацию, зафиксированную на магнитном носителе или передаваемую по телекоммуникационным каналам в форме, доступной восприятию ЭВМ.

Криминалистическая характеристика незаконного доступа к ЭВМ отличается от уже известных криминалистической науке преступных посятельств определенной спецификой. Важным элементом криминалистической характеристики незаконного доступа к ЭВМ являются сведения о личности правонарушителя.

Важным элементом криминалистической характеристики компьютерных преступлений является личность преступника. Субъект преступления - это минимальная совокупность признаков, характеризующих лицо, совершившее преступление, необходимых для привлечения его к уголовной ответственности. Именно личностные качества человека и внешняя среда в своем взаимодействии последовательно определяют мотивацию принятия решения относительно преступной деятельности в сфере использования компьютерных технологий. Мотивация включает процесс возникновения, формирования мотива преступного поведения и его цели. Мотив преступного поведения следует рассматривать как побуждение, сформировавшееся под влиянием социальной среды и жизненного опыта личности, которое является внутренней непосредственной причиной деятельности, и выражает личностное отношение к тому, на что направлена преступная деятельность [9].

Исследования проведенные Центром исследования компьютерной преступности показали, что возраст 33% злоумышленников на момент совершения преступления не превышал 20 лет; 54% - от 20 до 40 лет; 13% - были старше 40 лет [10].

Преступления связанные с незаконным доступом к ЭВМ в 5 раз чаще совершаются лицами мужского пола. Большинство субъектов таких преступлений имеют высшее или неоконченное высшее техническое образование (53,7%), а также другое высшее или неоконченное высшее образование (19,2%) [11]. Но в последнее время среди них постоянно увеличивается и доля женщин. Это связано с профессиональной ориентацией некоторых специальностей и рабочих мест ориентированными на женщин (секретарь, бухгалтер, экономист, менеджер, кассир, контролер и т.д.), оборудованных ЭВМ и имеющих доступ в сеть Интернет.

Проведенные исследования показали, что:

- 52% установленных правонарушителей имели специальную подготовку в области информационных технологий;

- 97% были сотрудниками государственных учреждений и организаций, использующие ЭВМ и информационные технологии в своей повседневной деятельности;

- 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники.

На основании вышеизложенного можно сделать следующие выводы:

Криминалистическая характеристика незаконного вмешательства в работу ЭВМ, отличается специфичной и включает в себя сведения о способе совершения и сокрытия преступления, данные о месте и времени преступного посягательства, данные о мотивах и целях совершенного деяния, а также сведения о личности преступника.

1. Способы совершения незаконного вмешательства в работу ЭВМ целесообразно подразделять на две группы: способы непосредственного доступа и удаленного доступа к ЭВМ. Существующие двух принципиально различным по своему характеру способов незаконного вмешательства в работу ЭВМ, каждый из которых обладает определенной спецификой, обуславливает особенности розыскной деятельности по каждому из них.

2. Информацию розыскного характера можно получить, изучая типичные способы противодействия расследованию по рассматриваемой категории дел. Основную информационную нагрузку несет способ сокрытия следов преступления. Сокрытие по преступлению связанным с незаконным вмешательством в работу ЭВМ - может выражаться в уничтожении, утаивании, маскировке, фальсификации как традиционно изучаемыми криминалистической способами (маскировка внешности, дача ложных показаний и т.д.), так и специфичные способы, связанными с компьютерным оборудованием и информацией (маскировка и фальсификация программных продуктов, маскировка местонахождения преступника при удаленном доступе к ЭВМ, восстановление нормальной работоспособности компьютеров и пр.).

Противодействие расследованию также может выражаться в воздействии на его участников либо уклонении от участия в расследовании.

3. Основными целями и мотивами совершения преступлений в сфере использования компьютерных технологий выступают корысть, материальные побуждения, месть, коммерческие цели или диверсия.

4. Незаконное вмешательство в работу ЭВМ в 5 раза чаще совершается мужчинами. Большинство субъектов преступления имеют высшее или неоконченное высшее образование, а также иное высшее или неоконченное высшее образование. Среди них преобладают лица в возрасте от 20 до 40 лет.

5. Розыскная деятельность следователя по делам о незаконном вмешательстве в работу ЭВМ представляет собой совокупность процессуальных и не процессуальных действий лица, производящего расследования, направленных на установление известных (следователя) объектов, имеющих значение для расследования по делу.

6. К числу основных объектов розыска по делам о незаконном вмешательстве в работу ЭВМ следует отнести: лиц, совершивших незаконное вмешательство; орудия, используемые для совершения незаконного вмешательства, компьютерную информацию, специальную литературу посвященную вопросам совершения незаконного вмешательства в работу ЭВМ и проблемам компьютерной безопасности.

7. В качестве розыскных признаков лиц, совершивших незаконное вмешательство в работу ЭВМ можно выделить общие признаки (пол, возраст, национальность, приметы, место жительства, профессия и пр.) и специальные признаки (обладание навыками в программировании, знании компьютерного оборудования, обладание определенным компьютерным оборудованием, данные оставленные преступником о самом себе в различных компьютерных системах и сетях и пр.).

8. Существует принципиальная возможность розыска компьютерного оборудования, использованного при совершении преступления.

При этом в качестве розыскных признаков могут выступать: конфигурация компьютера, использованного для совершения преступления; мобильность использованного компьютерного оборудования; наличие определенного сетевого или периферийного оборудования; установка на компьютере определенного программного обеспечения.

#### Литература:

1. Корж В.П. Теоретические основы методики расследования преступлений совершенных организованными преступными образованиями в сфере экономической деятельности. Монография - Харьков, 2002. - С. 107.
2. Шурунов Н.Г. Криминалистическая характеристика преступлений // Криминалистика (актуальные проблемы). Под ред. Е. И. Зуева. М., 1988. - С. 119.
3. Везов В.Б. Компьютерные преступления. Способы совершения, методики расследования. - М.: Право и закон, 1996. - С. 28.
4. В.Е. Козлов Теория и практика борьбы с компьютерной преступностью. - М. 2002. - С. 114.
5. Цимбалюк В.С. Личность компьютерной злочинності // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2001. - №3. - С.178.
6. Бельвин Р.С. Курс криминалистики. Том 3. М., 1997. С. 364.
7. Бельвин Р.С. Курс криминалистики. Том 2. М., 1997. С. 57.
8. Мухива А., Азаров Д. Про поняття злочинів у сфері комп'ютерної інформації // Право України. - №4. - Київ, 2003. - С.87.
9. Игошев К.Е. Типология личности преступника и мотивация преступного поведения. - Горький, 1974. - С.66.
10. Голубев В.А., Головкин А.Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий // [http://www.crim-research.org/library/New\\_g.htm](http://www.crim-research.org/library/New_g.htm)
11. Біленчук П. Д., Романчук Б. В., Цимбалюк В.С. та ін. Комп'ютерна злочинність. Навчальний посібник. - Київ: Атіка, 2002. - С.123.