4) целесообразность использования средств компьютерной техники в расследовании преступлений данной категории;

5) отсутствие методики расследования преступлений против информационной безопасности.

По оценкам отечественных и зарубежных исследователей, решение проблем раскрытия и расследования преступлений данного вида представляет собой задачу на несколько порядков сложнее, чем задачи, сопряженные с их предупреждением. «Именно корыстный мотив по соотношению с другими мотивами преступлений в сфере компьютерной информации составляет 66 процентов»[1], поэтому «…уровень латентности компьютерных преступлений определяется в настоящее время в 90 процентов. А из оставшихся 10 процентов выявленных компьютерных преступлений раскрывается только лишь один»[2].

Решением проблемы является выработка единых следственных действий, обязательных при расследований преступлений против информационной безопасности (на основе анализа и систематизации способов совершения преступлений против информационной безопасности с учетом комплексного исследования различных мнений в зарубежной литературе, складывающейся практики при расследовании данных видов преступлений). Важность таких исследований состоит в следующем:

данный вид преступления в рамках правового поля Республики Беларусь существует чуть более пяти лет;

отсутствуют систематизированные рекомендации по расследованию преступлений против информационной безопасности;

нет единого технологического и алгоритмизированного подхода к рассматриваемой проблеме;

в существующих литературных источниках можно наблюдать противоречивость рекомендаций, разноплановость и отсутствие полноты вопросов и обстоятельств, подлежащих разрешению в процессе расследования уголовных дел по совершению преступлений против информационной безопасности;

в настоящее время возникла необходимость формирования единого сбалансированного блока криминалистических технологий по всем видам преступлений, предусмотренных гл. 31 УК Республики Беларусь;

целесообразно формирование и балансирование интегративно-тактических комплексов и алгоритмов, которые отражают общую характеристику каждого вида преступления против информационной безопасности;

актуально выделение алгоритма допроса по каждому виду преступления против информационной безопасности, чтобы раскрыть систему обстоятельств, подлежащих доказыванию по каждому составу преступления;

целесообразно сформировать специфическую интегрированную тактику отдельных следственных действий по делам против информационной безопасности.

Решение данных задач приведет к выработке конкретной тактики и методики расследования преступления против информационной безопасности.

А.П. Леонов, *профессор кафедры административной деятельности и управления органами внутренних дел Академии МВД Республики Беларусь, кандидат философских наук, доцент;*
Н.Е. Щербак, *преподаватель кафедры уголовного права, процесса и криминологии ЧУО «БИП – Институт правоведения»*

К ХАРАКТЕРИСТИКЕ ПРИЧИННОГО КОМПЛЕКСА КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

С учетом потребностей практики предупреждения компьютерной преступности характеристику ее причинного комплекса целесообразно рассмотреть, во-первых, в контексте особенностей процессов глобализации и информатизации общества и его основных сфер (экономической, политической, социальной, духовной), оказывающих влияние на формирование причин и условий компьютерной пре-

[1] Панов В.П. Сотрудничество государств в борьбе с международными уголовными преступлениями. М., 1993. С. 67.
[2] Вехов В.Б. Указ. соч. С. 44.

ступности; во-вторых, в контексте создания причинного комплекса компьютерных преступлений на микроуровне, связанного с деформацией процесса социализации и появления у индивида криминогенной установки. Среди условий, способствующих компьютерной преступности на современном этапе развития информационного общества на постсоветском пространстве, могут быть названы следующие.

1. Отставание законодательно-правовой базы от темпов развития процессов информатизации общества, которое приводит к тому, что действия юридических и физических лиц в информационной сфере, наносящие материальный или моральный ущерб личности, обществу или государству, во многих случаях не получают должной правовой оценки и остаются безнаказанными, что в определенной мере стимулирует продолжение и расширение масштабов этих действий.

2. Информатизация денежного обращения, кредитных и банковских операций, а также финансового учета и отчетности, все большая ориентация потоков финансовой, экономической, таможенной, налоговой и другой информации в русло информационно-коммуникационных систем, распространенность безналичных расчетов за поставку оборудования, товары и услуги – все это делает данную сферу привлекательной для действий преступных групп и сообществ с целью извлечения материальной выгоды, хищения денежных средств и коммерческих секретов, а также для информационного шпионажа, шантажа и терроризма.

3. Рост компьютерного парка и как следствие этого – рост числа пользователей информационных технологий, увеличение объемов хранимой, обрабатываемой и передаваемой компьютерной информации. Возможность выхода отечественных пользователей в мировые информационные сети для обмена информацией, осуществления электронных платежей и др. Подобный обмен в настоящее время осуществляется самостоятельно, без контроля со стороны государственных органов, минуя географические и государственные границы.

4. Недостаточность мер по защите объектов информатизации, компьютерных систем и сетей, а также не всегда серьезное отношение руководителей к вопросу обеспечения защиты информации. Ряд организаций не принимает достаточных мер по обеспечению безопасности эксплуатируемых ЭВМ, их систем и сетей. Специалисты по информационной безопасности отмечают явное нежелание руководителей проводить работу и принимать меры по защите автоматизированных систем от неправомерного доступа. Как правило, отказ аргументируется нежелательными дополнительными ограничениями для пользователей и материальными затратами.

5. Наличие изъянов в программном обеспечении. Как показывает практика, большинство распространенных современных программных средств (в первую очередь операционных систем) не отвечает требованиям безопасности из-за изъянов в организации средств, отвечающих за безопасность, и различных «недокументированных» возможностей. После обнаружения многие изъяны ликвидируются с помощью обновления версий или дополнительных средств, однако то постоянство, с которым обнаруживаются все новые и новые изъяны, не может не вызывать опасений. Это означает, что большинство систем предоставляют злоумышленникам широкие возможности для осуществления нарушений.

6. Использование в преступной деятельности современных технических средств, в том числе компьютерной и телекоммуникационной техники. Более того, организованная преступность включена в широкомасштабный бизнес, выходящий за рамки отдельных государств, где без современной компьютерной и телекоммуникационной техники невозможно руководить и организовывать сферу незаконной деятельности. В настоящее время многие традиционные преступления невозможно совершать масштабно или без риска быстрого разоблачения, если не использовать высокие технологии, поэтому банковские сейфы все чаще опустошаются посредством неправомерного доступа в автоматизированные системы межбанковских расчетов, а магазины – через Интернет с помощью системы электронных платежей.

7. Снижение средней квалификации пользователей. Современные компьютеры за последние годы стали приобретать гигантскую вычислительную мощность, но стали гораздо проще в эксплуатации. Пользоваться компьютерами стало намного легче и все большее количество новых пользователей получает доступ к ним. Средняя квалификация пользователей снижается, что в значительной степени облегчает задачу злоумышленникам, так как большинство пользователей сами осуществляют администрирование личных рабочих станций. Большинство из них не в состоянии постоянно поддерживать безопасность своих систем на высоком уровне, поскольку это требует соответствующих знаний, навыков, а также времени и средств.

8. Небрежность в работе с информационными технологиями. Пользователи не всегда серьезно относятся к обеспечению конфиденциальности информации и часто пренебрегают элементарными требованиями по защите. Имеют место также упущения организационного характера: низкий профессионализм или отсутствие служб информационной безопасности, отсутствие должностного лица, отвечающего за режим секретности и конфиденциальность компьютерной информации; отсутствие договоров (контрактов) с сотрудниками о неразглашении конфиденциальной информации; недостаточное финансирование мероприятий по защите информации.

9. Низкий уровень специальной подготовки должностных лиц правоохранительных органов, в том числе и ОВД, которые должны предупреждать, раскрывать и расследовать неправомерный доступ к компьютерной информации и другие виды преступлений в этой сфере. В правоохранительных органах до последнего времени не было специальных подразделений, осуществляющих борьбу с компьютерной преступностью. Не хватает квалифицированных специалистов по расследованию преступлений в сфере высоких технологий, что заметно снижает активность обращений потерпевших от компьютерных преступлений за помощью в правоохранительные органы.

Глобальный аспект формирования причинного комплекса компьютерной преступности связан с процессом глобализации современного общества. Глобализация – это постепенное преобразование разнородного мирового социального пространства в единую глобальную систему, в которой беспрепятственно перемещаются информационные потоки, идеи, ценности и их носители, капиталы, товары и услуги, стандарты поведения и моды, видоизменяя миропредставление, деятельность социальных институтов, общностей и индивидов, механизмы их взаимодействия[1]. В сфере экономики глобализация проявилась в образовании таких финансовых организаций, как Международный финансовый фонд, Международный банк реконструкции и развития и др. Мощным ускорителем процесса глобализации стало создание и стремительное нарастание экономической мощи транснациональных корпораций (далее – ТНК). Образно говоря, сеть транснациональных корпораций составляет нервную и кровеносную систему глобальной экономики. По данным Н.Н. Моисеева[2], за последние несколько десятилетий возникли 37 тыс. ТНК, имеющих 200 тыс. филиалов в разных странах. Они владеют $^1/_3$ всех производственных фондов планеты, производят 40 % мирового продукта, осуществляют более половины внешнеторгового оборота (в том числе более 80 % торговли высокими технологиями), контролируют более 90 % вывоза капитала.

Сфера культуры также затронута процессом глобализации, поскольку в настоящее время вследствие развития средств связи наблюдается некоторая унификация стиля жизни. Культурная глобализация проявляет себя в процессе вестернизации, то есть распространения ценностей и норм, характерных для евро-американской культуры. Глобализация культуры осуществляется через распространение консьюмеризма (стратегии потребительства), который распространился по всему миру и заменил или дополнил более локализованные культуры. Стратегии потребительства распространяются через маркетинговую деятельность ТНК и средства массовой коммуникации. Технологические изменения в области телекоммуникаций также способствуют распространению однородной потребительской культуры.

Негативным компонентом глобализации является ее криминальное изменение, что находит свое проявление в росте компьютерной преступности. Глобализация имеет нелинейный характер, сопровождается усилением неравномерности социально-экономического развития, приводящим, с одной стороны, к возникновению пресловутого экономически процветающего «золотого миллиарда», а с другой – к маргинализации целого ряда стран, где люди находятся на грани выживания. Проявлением криминальной глобализации является и преступность, возникающая на «интернетовской почве», например, в виде вредоносных программ и спама[3]. Предпосылками-условиями компьютерной преступности на «интернетовской почве» являются реальные и потенциальные угрозы информационной безопасности, существующие со стороны виртуального сообщества хакеров. Одним из условий компьютерной преступности в настоящее время является низкий уровень обеспечения информационной безопасности большинства систем, подключенных к глобальной сети. Среди факторов, напрямую влияющих на уровень безопасности инфокоммуникационных систем, особое место занимает коммер-

[1] См.: Бабосов Е.М. Общая социология. Минск: ТетраСистемс, 2002. С. 494.

[2] См.: Моисеев Н.Н. Судьба цивилизации. Путь разума. М.: МНЭПУ, 1998. С. 149.

[3] Вредоносная программа – программа (часть программы), которая заведомо приводит к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, их системы или сети. Спам – сообщения электронной почты рекламного или иного характера, рассылаемые адресатам, которые не выразили в явной или неявной форме желания получать такие сообщения либо выразили нежелание их получать.

ческое программное обеспечение (далее – ПО), для которого большое количество опций и быстрый вывод на рынок часто имеют большее значение, чем его безопасность. Разработчиками, взломщиками и независимыми исследовательскими группами постоянно выявляются ошибки в таком ПО. Распространение коммерческих продуктов в глобальном масштабе означает, что, как только обнаружена уязвимость, взломщик может многократно использовать ее на миллионах систем, на которых установлен недоработанный в плане безопасности продукт.

Микроуровень формирования причинного комплекса компьютерной преступности связан с дефектами социализации индивида, приводящими к формированию у него криминогенной установки. Важнейшими элементами процесса социализации являются:

социальная среда с ее многообразными сферами;

человек как деятель с его природными задатками, его предметная деятельность с ее механизмами;

круги общения человека, выраженные в структуре его социальных ролей, содержание, структура, направленность его сознания;

субъект социализации с его механизмами идеологического, педагогического, нравственного, эстетического и других видов воздействия на мышление и поведение социализирующегося человека.

Игра – форма социализации индивида. Компьютерные игры при злоупотреблении ими могут вызвать деформацию социализации индивида. Рынок игровых программ бурно развивается. Его оборот уже сейчас оценивается миллиардами долларов в год и продолжает расти. Компьютерная игромания создает питательную среду для формирования компьютерных фанатов – игроманов, хакеров, крэкеров.

Для криминологии первостепенное значение приобретает изучение закономерностей деформации процесса социализации человека в различных условиях, в различные периоды жизни и деятельности человека, приводящие к формированию у индивида криминогенной установки. На формирование криминогенной установки индивида большое значение оказывает виртуальное сообщество хакеров в Интернете, играющее для индивида роль референтной группы[1].

Анализ интернет-ресурсов хакеров показывает, что в настоящее время компьютерный андеграунд представляет собой виртуальное сообщество, располагающее в Интернете значительными информационными и интеллектуальными ресурсами и механизмами самоорганизации деятельности[2]. Широко распространены в Интернете электронные издания хакерских советов и рекомендаций, а также каталоги хакерских утилит по взлому компьютерных систем и сетей. Уже сейчас в Интернете известно более 120 хакерских сайтов деструктивной направленности. Кроме этого издаются многочисленные журналы для хакеров, являющиеся носителями хакерской субкультуры.

В заключение отметим, что приведенная характеристика причинного комплекса компьютерной преступности отражает ее текущее состояние и тенденции развития и представляет актуальность для практики ее предупреждения.

***И.И. Лузгин**, старший преподаватель кафедры уголовного права и криминалистики Полоцкого государственного университета, соискатель НПФ Академии МВД Республики Беларусь*

СОВРЕМЕННЫЕ АСПЕКТЫ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Найти на месте происшествя, грамотно изъять и направить на исследование с целью получения результата можно только те следы, которые соответствуют уровню познаний специалиста и всех участников осмотра. Недополученные исходные данные осложнят решение последующих задач. Это требует внимательного отношения к организации, проведению и криминалистическому обеспечению первичных следственных действий и всех видов осмотров мест происшествий. Именно объективные

[1] Референтная группа – это реальная или воображаемая социальная общность, на нормы, ценности и мнение которой индивид ориентируется в своем поведении.

[2] См.: Полещук М.И., Щербак Н.Е. Информационные ресурсы взломщиков в Интернете // Упр. защитой информ. 2003. Т. 7. № 1. С. 114–122.