ция самодельного ВУ, место заложение заряда); место совершение преступления, способ, личность потерпевшего могут указать на мотив преступления (корыстный, хулиганский, из мести, террористический акт).

Все обнаруженные следы и вещественные доказательства фиксируются путем описания в протоколе осмотра места происшествия с указанием формы, размера, цвета, вида материала, а также положения на месте. Местонахождение обнаруженных следов и предметов отмечается на план-схеме. По окончании фиксации все обнаруженные на месте происшествия следы и предметы изымаются и упаковываются с соблюдением требований Уголовно-процессуального кодекса.

Описание обнаруженных объектов в протоколе требует не только скрупулезности, но и привязки к устойчивым ориентирам на месте. Поскольку при осмотре большинства мест происшествий один из ориентиров определяется достаточно точно – это эпицентр взрыва, часто для фиксации применяется метод угловых координат. Его разновидностью считается так называемый способ циферблата часов [5, с. 463]. Направление на 12 ч совмещается с показанием стрелки на север, и все фиксируемые объекты отмечаются по расстоянию до эпицентра и по угловому отклонению по циферблату. При отсутствии четко выраженного центра взрыва рекомендуется использовать метод базовой линии, суть которого заключается в отметке на месте осмотра прямой линии путем прочерчивания или натягивания шнура с делениями определенного шага. Местонахождение объекта фиксируется кратчайшим по перпендикуляру расстоянием до шнура с отметкой на нем и расстоянием от этой отметки до начала базовой линии [3, с. 67].

Вышеизложенное позволяет сделать следующий вывод:

осмотр места происшествия, связанный с использованием ВУ, имеет свои особенности, связанные с повышенной опасностью для жизни и здоровья его участников, большими площадями и территорией, на которых совершено преступление; разрушениями конструкций и коммуникаций; привлечением к участию в следственном действии большого количества специалистов; необходимостью совмещать осмотр с проведением пожарных, спасательных и восстановительных работ, а также оказанием помощи пострадавшим. Данные особенности обусловлены способом совершения преступления и механизмом следообразования.

Библиографические ссылки

1. Беляков, А.А. Криминалистическая теория и методика выявления и расследования преступлений, связанных со взрывом : дис. … д-ра юрид. наук : 12.00.09 / А.А. Беляков. Екатеринбург, 2003.

2. Дильдин, Ю.М. Из практики экспертного исследования объектов, обнаруженных после взрыва самодельного устройства / Ю.М. Дильдин, А.И. Колмаков, С.И. Тетерев // Эксперт. практика. 1982. № 19.

3. Михайлов, М.А. Криминальный взрыв: возможности расследования / М.А. Михайлов. М. : Юрлитинформ, 2004.

4. Пантелеев, И.Ф. Расследование и профилактика взрывов, пожаров, крушений и авиапроисшествий / И.Ф. Пантелеев. М. : Юрид. лит., 1975.

5. Разумов, Э.А. Осмотр места происшествия: методика и тактика / Э. А. Разумов, Н.П. Молибога. Киев : МВД Украины, 1994.

О.О. Петрухин, *начальник отделения УРПСВТ*
МВД Республики Беларусь

ЛИЧНОСТНАЯ ХАРАКТЕРИСТИКА ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

Рассматривается личностная характеристика преступника, совершающего компьютерные преступления, приводится его классификация на отдельные группы и подгруппы с целью определения характерных особенностей личности и их корреляционной связи со способами совершения противоправных деяний. Указывается на необходимость построения практически значимых типовых моделей различных категорий компьютерных преступников, необходимых для эффективного распределения сил и средств, с целью установления правонарушителя.

Личностная характеристика преступника является важной составляющей обобщенной информационной модели преступления. Она коррелируется со способом совершения преступления, особенностью следовой информации о нем. С прикладной точки зрения собранные в процессе раскрытия преступления сведения о личности преступника, его криминальном поведении и виновности создают фактическую базу для принятия обоснованных правовых решений по его уголовному преследованию.

Одним из главных факторов изучения и анализа личности преступника, совершающего компьютерные преступления, является рост данных видов преступлений и принятия мер для борьбы с ними.

Так, если в 2003 г. было совершено 118 преступлений в сфере высоких технологий, то в 2005 г. – 178, в 2007 г. – 996, в 2008 г. – 1614 (+62 %). Анализ показывает стремительный рост компьютерных преступлений, при этом около 90 % составляют хищения с использованием компьютерной техники.

Анализ специализированной научной литературы позволяет сделать вывод о существовании двух специфических направлений деятельности по формулированию личностной характеристики лиц, совершающих компьютерные преступления [3, с. 161]. Первое предусматривает получение данных о личности неизвестного преступника по оставленным им следам на месте преступлений, в памяти свидетелей и по другим источникам. Чаще всего такая информация дает представление об общих свойствах какой-то группы лиц, среди которых может находиться преступник. Второе предусматривает изучение личности подозреваемого или уже известного обвиняемого с целью исчерпывающей оперативной оценки личности субъекта.

Из существующих типологизаций компьютерных правонарушителей концептуальный характер носят следующие.

1. Типологизация В.В. Крылова (лица, осуществляющие неправомерный доступ к компьютерной информации в группе по предварительному сговору или организованной группой; лица, осуществляющие неправомерный доступ к компьютерной информации с использованием своего служебного положения; лица, имеющие доступ к ЭВМ, но осуществляющие неправомерный доступ к компьютерной информации или нарушающие правила эксплуатации ЭВМ; лица, создающие, использующие и распространяющие вредоносные программы) [4, с. 64].

2. Типологизация В.Б. Вехова и В.Е. Козлова (лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности; лица, страдающие новым видом психических заболеваний – информационными болезнями или компьютерными фобиями; профессиональные компьютерные преступники с ярко выраженными корыстными целями) [2, с. 38–39; 3, с. 162; 8, с. 234, 239].

Полагаем, что вторая типологизация носит ярко выраженный прикладной характер и может быть использована в качестве основы для детальной характеристики рассматриваемой группы лиц.

1. Лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности.

Хакеры – компьютерные хулиганы, проникающие в память чужих компьютеров с помощью своих подключенных по телефонным каналам к сетям передачи данных. При этом преследуются разнообразные цели: от любопытства и удовлетворения тщеславия до получения конкретной выгоды. Одним из основных внешнеповеденческих признаков хакерства является безразличие ко всему, что не имеет непосредственного отношения к работе с компьютером. У хакеров атрофирована установка на конечный результат, их не интересует полезность и возможность передачи продукта их деятельности в общественное пользование. Вследствие этого они игнорируют общественные интересы и проявляют «компьютерный снобизм» [3, с. 163]. Мотивы поступков различны. Как правило, это хулиганские побуждения, реже – исследовательский интерес. В свою очередь, хакеров можно классифицировать с учетом сферы интересов и специализации группы: собственно хакеров, наемных хакеров, информационных брокеров и метахакеров [5, с. 49].

Собственно хакеры – профессионалы, досконально знающие компьютеры и программирование, умеющие нестандартно мыслить и добиваться результатов, используя нетрадиционный, оригинальный подход к проблеме. Для них основными мотивами деятельности являются не деньги, а преодоление технических барьеров и чувство собственного превосходства. Они настороженно относятся к властям, считая, что любое вторжение властей разрушает самоуправляемый мир тех, кто обитает в интернете. «Классические» хакеры ищут только морального удовлетворения. Они проникают в компьютеры и программы только для того, чтобы показать свои возможности, не причиняя вреда окружающим. Основной лозунг хакерского движения – «Информация должна быть бесплатной и общедоступной». Хакеры с большим энтузиазмом изучают функционирование компьютеров и программ, для чего порой забираются в запретные области.

О наемных хакерах говорят в тех случаях, когда хакер ловит хакера. Этот вид деятельности и не был известен в мире киберпространства до тех пор, пока ФБР не начала нанимать хакеров для того, чтобы они помогали в расследованиях компьютерных преступлений и атак через интернет. Сегодня боязнь незаконных вторжений через интернет заставляет некоторые компании нанимать сторонних специалистов – известных хакеров – для работы по защите и проверке безопасности своих компьютерных систем.

Метахакеры являются своего рода паразитами на паразитах. Они отслеживают работу обыкновенных хакеров, оставаясь незамеченными, и пользуются результатами их труда.

Информационные брокеры делают хакерам заказы на кражу информации, а затем перепродают ее иностранным правительствам или конкурирующим коммерческим организациям. Наносимый ими ущерб измеряется не только в долларах, они представляют собой угрозу национальной безопасности, поскольку шпионаж с использованием интернет-технологий становится обычным явлением, а количество хакеров, занимающихся им, стремительно растет.

Крэкеры осуществляют, как правило, взлом программ, генерацию кодов, взлом программно-аппаратных средств защиты на программном уровне с целью получения информации, нанесения ущерба и иными корыстными целями. Они являются программистами высокого класса и в отличие от хакеров могут стереть или изменить данные в соответствии со своими интересами. Крэкеров можно подразделить на вандалов, шутников, взломщиков, пиратов.

Вандалы являются самой известной и в то же время самой малочисленной частью крэкеров. Их главная цель – взломать систему для ее дальнейшего разрушения. Эта стадия обычна характерна для новичков.

Шутники – наиболее безобидная часть крэкеров. Своей известности они добиваются путем взлома компьютерных систем и внесения туда различного рода юмористических эффектов. К шутникам также можно отнести создателей вирусов с различными визуально-звуковыми эффектами (музыка, дрожание или переворачивание экрана, рисование всевозможных картинок и т. д.). Шутники обычно не наносят существенного ущерба компьютерным системам и их администраторам.

Взломщиками являются профессиональные крэкеры, которые пользуются наибольшим почетом и уважением в своей среде. Их основной задачей является взлом компьютерной системы с целью кражи или подмены хранящейся там информации.

Пираты воруют свежие программы с помощью средств, самостоятельно разработанных или заимствованных у взломщиков, и обладают определенной специализацией:

пираты-взломщики взламывают компьютерную защиту;

пираты-курьеры копируют ворованное программное обеспечение на свой компьютер;

пираты-дистрибьюторы занимаются распространением ворованного программного обеспечения [7, с. 13]. Например, гражданин А. в период с января по октябрь 2006 г. с использованием вредоносной программы Sable осуществлял взлом программы определения аппаратного ключа защиты от несанкционированного доступа, входящей в состав программного обеспечения «1 С: Бухгалтерия». Возбуждены уголовные дела по признакам состава преступления, предусмотренного ч. 1 ст. 354, ч. 1 ст. 350.

Принципиальное различие между хакерами (hackers) и крэкерами (crackers) состоит в целях, которые они преследуют.

Основная задача хакера состоит в том, чтобы, исследуя вычислительную систему, обнаружить слабые места (уязвимость) в ее системе безопасности и информировать пользователей и разработчиков системы с целью последующего устранения найденной уязвимости.

Основной задачей крэкера является непосредственное осуществление взлома системы с целью получения несанкционированного доступа к чужой информации, ее хищения, подмены или объявления факта взлома. Крэкер по своей сути ничем не отличается от обычного вора, взламывающего чужие квартиры и крадущего вещи, он взламывает средства компьютерной техники и похищает информацию.

Общими признаками для указанных подгрупп являются:

завышенная оценка своих профессиональных и интеллектуальных способностей;

использование специфического жаргона не только в кругу специалистов, но и при повседневном общении;

отсутствие интереса к проблемам повседневной жизни и др.

Для рассмотренных подгрупп следует указать особенности, свидетельствующие о совершении компьютерного преступления лицами, входящими в них:

отсутствие целеустремленной, продуманной подготовки к преступлению;

оригинальность способа совершения преступления;

непринятие мер к сокрытию преступления;

совершение озорных действий на месте происшествия [2, с. 40].

2. Касаясь характеристики преступников, отнесенных ко второй группе, следует отметить, что Всемирная организация здравоохранения, обобщив материалы о влиянии компьютеров на здоровье человека, пришла к выводу, что частая и продолжительная работа на компьютере несет негативные

последствия для здоровья человека, прежде всего психического. Это выражается в быстрой утомляемости, скачкообразных изменениях артериального давления, повышенном потовыделении, глазных стрессах, головных болях, обмороках [1, с. 216].

Понятие интернет-зависимость как психического расстройства, навязчивого желания подключиться к интернету и болезненной неспособности вовремя отключиться от интернета впервые в 1995 г. было описано доктором И. Голдбергом, который выделял следующие основные симптомы данного расстройства:

использование интернета вызывает болезненное негативное стрессовое состояние или дистресс;

использование интернета причиняет ущерб физическому, психологическому, межличностному, экономическому или социальному статусу.

В 1997–1998 гг. вышли первые монографии по проблеме интернет-зависимости (К. Янг, Д. Гринфилд).

В 2005 г. членом-корреспондентом Международной академии наук педагогического образования, кандидатом педагогических наук, доцентом В.А. Плешаковым введено понятие киберсоциализации человека как процесса качественных изменений структуры личности, происходящих в результате социализации человека в киберпространстве интернет-среды, то есть в процессе использования его ресурсов и коммуникации с «виртуальными агентами социализации», встречающимися человеку в интернете.

Он отмечает значительное количество негативных последствий – технострессов, компьютерофобий, кибераддикций, то есть почти наркотическую зависимость от игровых программ и интернета, сужения круга интересов, некоммуникабельность и социальный аутизм как следствие патологической поглощенности использования и применения информационных технологий. Человек в виртуальном мире не ограничивается позицией зрителя, а включается в действие и сам влияет на происходящие процессы, вследствие чего теряется его связь с реальным миром. Как следствие – интернет-зависимость ведет к социальной изоляции, увеличивающейся депрессии, распаду семьи, неудачам на работе или в учебе, финансовому неблагополучию.

В настоящее время можно выделить следующие типы интернет-зависимости:

1. Игровая зависимость, или игромания – навязчивая игра в компьютерные игры. В данном случае игра дает способность отойти от той социальной роли, к какой человек привык и в какой его привыкли видеть окружающие. Для игромана реальный мир становится неинтересным и полным опасностей, так как большинство из них – это люди, которые плохо адаптируются в социуме. В виртуальном мире человеку все разрешено и он устанавливает свои правила игры. Для игромана характерны следующие симптомы:

ежедневно, без пропусков, играет на компьютере;

после начала игры теряет чувство времени;

не хочет оставлять игру незавершенной;

не признает, что слишком много времени проводит за игрой на компьютере;

окружающие начинают упрекать его в том, что он проводит много времени у монитора;

не прекращает игру, когда достигнут какой-то уровень сложности, играет дальше;

сравнивает свои результаты со старыми и гордится этим, сообщает об этом всем, кому можно;

играет вместо посещения занятий, в разгар работы.

2. Навязчивый серфинг или информационная перегрузка – заключается в бесконечном путешествии по сети интернет, поиске информации по базам данных и поисковым сайтам.

3. Виртуальное общение и знакомство в сети интернет, переписка на форумах и в чатах.

4. Просмотр порносайтов и киберсекс.

5. Посещение интернет-магазинов, интернет-аукционов и азартных игр.

Одной из причин формирования компьютерных преступников может заключаться в том, что интернет-зависимость отрицательно влияет на формирование личности и ведет к ряду нежелательных последствий: снижаются волевые качества, возникает иллюзия вседозволенности, разрушается психика. Аномальные изменения психики накладывают отпечаток на личностные качества субъекта, что может послужить толчком к совершению преступления.

Для данной категории лиц характерно:

непринятие простейших мер по сокрытию факта общественно опасного деяния;

отсутствие целенаправленной предварительной подготовки к его совершению;

внезапность, безмотивность общественно опасных действий.

К третьей группе, по мнению Ю.М. Батурина, относятся лица, имеющие доступ к ЭВМ и их сетям в связи с исполнением своих профессиональных или служебных обязанностей либо хорошо владеющие вычислительной техникой [1, с. 217–246]. При этом преступники могут различаться как по уровню профессиональной подготовки, так и по социальному положению. При изучении особенностей данной группы следует отметить, что совершение преступлений в сфере информационной безопасности не является для них формой самореализации. Для них совершение криминальных деяний в этой сфере является противоправным бизнесом. К данной группе лиц можно отнести фрикеров и кардеров.

Фрикеры – лица, специализирующиеся на совершении преступлений в области электросвязи с использованием компьютерной информации и специальных технических средств, разработанных для негласного получения информации с технических каналов. Основным направлением их преступной деятельности является хищение и генерирование телефонных карточек и номеров доступа с целью переноса платы за телефонные разговоры на счет другого абонента; клонирование сим-карт; несанкционированное подключение к телефонным линиям других абонентов (например, гражданин Б. в период с марта 2005 г. по апрель 2006 г. в салоне сотовой связи и по месту жительства посредством персонального компьютера и универсального программатора, с использованием вредоносных программ осуществлял несанкционированный доступ к информации, хранящейся на машинных носителях операторов сотовой связи Республики Беларусь. Возбуждены уголовные дела по признакам состава преступления, предусмотренного ч. 2 ст. 349, ч. 1 ст. 354).

Кардеры – лица, специализирующиеся на хищениях денежных средств с использованием поддельных банковских пластиковых карт или их реквизитов (например, гражданин В. в период с ноября 2006 г. по февраль 2007 г. по месту жительства с использованием компьютерной техники и интернета завладел 10 500 долларами США гражданки г. Минска. Возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 3 ст. 212).

Для данной категории лиц характерны следующие особенности:

подготовка к осуществлению противоправных деяний;

противоправные деяния совершаются в большинстве случае в группе и с распределением ролей;

многократность осуществления преступных действий;

наличие специальных знаний [6, с. 75].

Основными мотивами у лиц, отнесенных к третьей группе, являются:

корысть;

политические цели;

месть [3, с. 167].

Завершая рассмотрение личности преступника, совершающего компьютерные преступления, необходимо отметить, что построение практически значимых типовых моделей различных категорий компьютерных преступников, знание основных черт этих людей позволит оптимизировать процесс определения круга лиц, среди которых целесообразно вести поиск преступника, тем самым эффективнее распределяя силы и средства, необходимые для установления правонарушителя.

Библиографические ссылки

1. Батурин, Ю.М. Проблемы компьютерного права / Ю.М. Батурин. М. : Юрид. лит., 1991.

2. Вехов, В.Б. Компьютерные преступления. Способы совершения, методики расследования / В.Б. Вехов. М. : Право и закон, 1996.

3. Козлов, В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. М. : Горячая линия – Телеком, 2002.

4. Крылов, В.В. Информационные компьютерные преступления : учеб. и практ. пособие / В.В. Крылов. М. : НОРМА-ИНФРА-М, 1997.

5. Леонов, А.П. Комплексная защита автоматизированных систем правоохранительных органов от несанкционированного доступа / А.П. Леонов, Г.В. Фролов // Компьютерная преступность: состояние, тенденции и превентивные меры ее профилактики : тезисы докл. СПб. : С.-Петерб. ун-т МВД России, 1999.

6. Лепёхин, А.Н. Расследование преступлений против информационной безопасности / А.Н. Лепёхин. Минск : Тесей, 2008.

7. Масленченко, С.В. Субкультура хакеров как порождение информатизации общества : автореф. дис. … канд. юрид. наук : 24.00.01 / С.В. Масленченко ; С.-Петерб. гос. ун-т. СПб., 2008.

8. Полевой, Н. Компьютерные технологии в юридической деятельности : учеб. и практ. пособие / под ред. Н. Полевого, В. Крылова. М. : БЕК, 1994.