УДК 343.918.2

МАСЛАКОВА Е.А.

Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика

В статье рассматриваются существующие в юридической науке подходы к определению дефиниций “компьютерный преступник”, “хакер”. С точки зрения уголовно-правовой и криминологической науки анализируются особенности, значимые для эффективной борьбы с подобными преступниками.

Ключевые слова: компьютерное преступление, компьютерный преступник, информационное преступление, хакер, сфера компьютерной информации, защита компьютерной информации, информационные технологии.

Изучение особенностей лиц, совершающих преступления, является важным условием правильной организации борьбы с определенным видом преступной деятельности. Для преступлений, связанных с использованием компьютерных технологий, изучение личности преступника приобретает особую актуальность, так как в данном случае приходится сталкиваться с субъектами, которые до недавнего времени не попадали в поле зрения правоохранительных органов. Любопытство общества по отношению к этим новым видам преступлений отчасти затеняет связанную с ними опасность, порождает отношение к компьютерным преступникам как к экзотическому явлению, формирует их искаженные образы, не соответствующие действительности. Поэтому для восстановления реальной картины необходимо уделить внимание особенностям таких лиц, вероятным мотивам преступления, поведенческим признакам, проявляющимся при подготовке и совершении преступлений.

Анализ уголовных дел, а также специальной литературы позволяет констатировать, что подобные преступления в подавляющем большинстве совершаются лицами мужского пола. Однако, принимая во внимание тенденции в мировой практике, можно предположить, что скоро доля женщин в такого рода преступлениях будет увеличиваться[1].

Важнейшим компонентом криминологического портрета компьютерного преступника является возраст, который, несомненно, накладывает свой отпечаток на поведение людей, их потребности и жизненную установку.

Среди преступников данного типа преобладают молодые люди в возрасте от 18 до 24 лет (52% изученных уголовных дел), т.е. возраст студенческой молодежи либо тех, кто окончил вуз, но еще не вступил в брак, возраст первого серьезного карьерного роста. Иными словами, это едва ли не самый важный период социализации человека в обществе, особенно для мужчин, требующий сил, времени и разного рода ресурсов. Именно в этом возрасте у таких лиц особенно высока потребность в самоутверждении и стремление получить максимальное количество жизненных благ при отсутствии реальной возможности достичь этого.

Однако, на наш взгляд, полученные в результате анализа уголовных дел данные не всегда отражают реальное состояние

дел, так как в данном случае мы имеем дело только с выявленными правонарушениями. В то же время официальные власти большинства стран, в том числе и США, где подобные преступления расследуются с 1966 года, вынуждены признавать, что выявление правонарушителя в 90% случаях невозможно. По нашему мнению, наиболее опасные преступления подобного вида совершают лица в возрасте от 25 до 35 лет, имеющие техническое образование и продолжительный опыт работы в области информационных технологий, неправомерная деятельность которых практически никогда не бывает наказана. Основная же часть раскрытых компьютерных преступлений совершается специалистами невысокой квалификации, знаний которых не хватает для того, чтобы скрыть следы своего преступления.

В последнее время прослеживается тенденция к омоложению компьютерных преступников, что может привести к тому, что в скором времени доля и общественная опасность хакеров, не достигших 16-летнего возраста, будет усиливаться по мере роста компьютеризации общества[2]. Среди причин такого омоложения можно отметить потребность в общении в Интернете, в обретении друзей из сетевого сообщества.

Важное значение для выявления подобных лиц имеет также определение психологических особенностей их личности. При этом важно не описание всех качеств личности, а выделение ведущих, определяющих характер поведения.

Как правило, изучаемые лица имеют замкнутый характер, склонны к депрессии, погружены в личные переживания, не стремятся достичь высокого положения в обществе. Большинство хакеров склонны к индивидуальным формам деятельности, в общении для них характерны холодность, конфликтность и пониженная эмоциональность.

Несмотря на это, многие из них имеют ярко выраженную потребность принадлежать к определенной большой социальной группе, и такая потребность находит реализацию при объединении их в хакерские сообщества.

По мнению специалистов, среди наиболее распространенных качеств таких преступников преобладают правовой нигилизм и завышенная самооценка. Гипертрофированная самооценка приводит к тому, что отдельные лица совершают противоправные деяния спонтанно, без серьезной предварительной подготовки. Под воздействием “комплекса безнаказанности” они оставляют многочисленные послания руководителям служб безопасности, с гордостью публикуют сообщения о своих противоправных действиях в сетевых конференциях и т.п. По результатам опросов, проведенных ФБР, до 98% хакеров считают, что их никогда не смогут уличить в хакерстве[3].

Также необходимо отметить, что эти люди, как правило, являются яркими, мыслящими личностями. Для многих из них характерны достаточный уровень квалификации, глубокие познания в области информационных технологий, высокая работоспособность, упорство. Эти сами по себе позитивные качества при выборе субъектом преступных способов достижения целей становятся элементами преступного профессионализма. В частности, высокий интеллект и профессиональная подготовленность позволяют преступнику достаточно полно оценить все возможные препятствия на пути достижения поставленных целей и выбрать оптимальный вариант поведения, просчитав вероятные действия правоохранительных органов.

Среди поведенческих признаков таких лиц могут быть выделены: поддержание связей с хакерскими группами; обсуждение способов совершения преступлений; регулярное участие в конференциях хакерской направленности; заявления о совершении правонарушений; использование специфического жаргона.

Проблема получения информации о типичных характеристиках личности преступника, совершающего преступления рассматриваемой категории, усугубляется отсутствием достаточного объема эмпирического материала для проведения ее всестороннего анализа.

В настоящее время совокупность лиц, совершающих преступления в сфере информационных технологий, является достаточно разнородной по своему составу. Поэтому стремление построить единый

обобщенный портрет всех личностей, совершающих противоправные действия в данной сфере, обречено на неудачу. Тем не менее выделение категории лиц, совершающих подобные преступления, на основе различных критериев способствует выявлению объединяющих их особенностей.

Например, канадский психолог М. Роджерс выделил группы преступников в зависимости от уровня их технической подготовленности: новички; кибер-панки; свои – служащие организаций-жертв; кодировщики; хакеры старой гвардии; профессиональные преступники; кибертеррористы[4].

Д. Айков делит компьютерных преступников в зависимости от мотивов преступления на три категории: взломщики (основное побуждение – проникновение в систему), преступники (основное побуждение – выгода), вандалы (основное побуждение – нанесение ущерба)[5].

Представляет несомненный интерес и деление, представленное в Указе президента США, направленном на борьбу с компьютерной преступностью. Здесь обозначены три основные группы субъектов: неорганизованные субъекты (сотрудники организаций, хакеры); организованные субъекты (представители организованной преступности, промышленного шпионажа, террористы); представители спецслужб других государств[6].

По мнению многих сотрудников правоохранительных органов западных стран, недовольные служащие и недавно уволенные сотрудники, достаточно подготовленные в области информационных технологий и по роду деятельности имеющие определенные права доступа к вычислительным системам, составляют наиболее значимую в процентном отношении группу киберпреступников. Имеются примеры, когда обиженные увольнением служащие наносили серьезный ущерб функционированию компаний.

Например, в 2002 г. один из бывших сотрудников фирмы UBS PaineWebber нанес ей ущерб на сумму около 3 млн. долл. Он внедрил в сеть организации через заблаговременно оставленную дыру в программном обеспечении вредоносную программу. Из 1,5 тыс. компьютеров компании было повреждено почти две трети. Злоумышленник предполагал получить прибыль за счет падения курса акций компании.

Достаточно большую потенциальную опасность представляют и лица из числа штатных сотрудников: системные программисты, сетевые администраторы, специалисты по защите информации, операторы ЭВМ, инженерный персонал, пользователи системы. Наиболее опасен в этом отношении специалист по защите информации, в силу своих профессиональных навыков способный умело скрыть преступление, а на случай обнаружения имитировать проникновение злоумышленника извне. В целом в правоохранительной практике сотрудников пострадавшей организации принято считать основным субъектом противоправных действий в отношении сетевых объектов.

Однако в последние годы ситуация постепенно меняется. В отчете ФБР и Института компьютерной безопасности США в качестве основного источника опасности для объектов вычислительной техники называются внешние подключения к сети Интернет (в 2012 г. — 89% инцидентов; в 2011 г. – 80%; в 2010 г. – 67%). Аналогичные оценки приводятся и в обзоре, подготовленном Конфедерацией британской промышленности (Confederation of British Industry). Утверждается, что основная угроза исходит не от работников компании, а в большей степени от хакеров, а также от уволенных сотрудников и представителей организованной преступности[7].

Для российского общества проблема участия представителей технической элиты в противоправной деятельности связана и с определенными социальными предпосылками. По мнению специалистов, вероятность совершения сетевых преступлений повышается в тех регионах, где имеется множество подготовленных профессионалов, не получающих соответствующего своим способностям вознаграждения за свою работу.

Серьезную угрозу информационной безопасности могут нести конкуренты или лица, занимающиеся промышленным шпионажем, а также профессиональные преступники и кибертеррористы. Представители этих групп осуществляют противоправную деятельность в широком диапазоне –

от корпоративного шпионажа до чрезвычайно опасных диверсий против вычислительных систем жизненно важных объектов. Такие лица, как правило, хорошо обучены и имеют доступ к самому современному оборудованию.

Между тем для сотрудников правоохранительных органов особый интерес, как правило, представляют лица, которые могут совершать неочевидные опасные преступления. В этом отношении именно хакеры как группа, продуцирующая большое число латентных преступлений, выступают достаточно новым и важным в криминологическом плане явлением. Специалисты достаточно высоко оценивают угрозу сетевой безопасности, исходящую от хакеров, которые представляют определенный криминологический феномен, требующий соответствующего осмысления.

Следует отметить, что, несмотря на частое использование термина "хакер", среди специалистов до сих пор отсутствует его единое толкование. Этот термин используется, как минимум, в двух значениях. Первое имеет негативную окраску, определяет личность с противоправными установками, преступника, компьютерного "взломщика"; второе вполне позитивно и подразумевает специалиста в области информационных технологий, профессионала, увлеченного своим делом[8].

Конечно, не стоит ставить знак равенства между хакерами и преступниками, к сообществу хакеров следует относиться как среде, оказывающей существенное влияние на преступность в сфере высоких технологий. В то же время не все виды девиантного поведения в сфере компьютерной информации связаны с хакерами (этот термин более узок, чем "лицо, совершающее преступление в сфере компьютерной информации"). Но так или иначе, именно хакеры являются ядром компьютерной преступности, породившим соответствующую субкультуру[9].

Хакерская среда образует уникальное явление, не имеющее аналогов в правоохранительной практике и лишь по отдельным характеристикам приближающееся к другим криминальным сообществам. Одно из его основных отличий связано с использованием коммуникационных возможностей современных глобальных сетей для обсуждения и координации своей деятельности. С этой целью в глобальных сетях организуются конференции хакерской тематики, создаются хакерские сайты.

Хакерская среда имеет сложную организацию, находится в процессе постоянного развития и еще достаточно слабо изучена. Изучение хакерского сообщества затруднено в связи с явной недостаточностью фактических документированных материалов, отсутствием возможности обычного статистического наблюдения. Это заставляет прибегать к методам косвенного познания, например выявлению и опросу жертв правонарушений, специалистов по защите информации, изучению документов и т. д. Важным источником исходной информации для анализа выступают данные зарубежных исследователей. Представляется эффективным и еще один из методологических приемов: контент-анализ основных каналов общения хакеров – электронных досок объявлений, сайтов криминальной направленности, конференций.

При изучении хакерской субкультуры следует помнить, что она формировалась главным образом в киберпространстве в условиях отсутствия государственных границ и государственного регулирования совершаемых в нем действий. Анализ норм хакерской этики делает очевидным игнорирование основных правовых принципов. Отдельным слоям общества импонирует идеология хакеров, которая сконцентрирована вокруг лозунгов: "информация принадлежит всем", "программы должны быть общедоступными и не должны защищаться авторским правом". Как следствие, снисходительное отношение к хакерам переносится и на совершаемые ими преступления[10].

Вполне естественно, что в таких условиях хакеры ощущают себя особым элитарным сообществом с определенными законами, традициями, солидарностью, поэтому большинство из них причиняют ущерб сетевым объектам в стремлении поддержать такой мнимый престиж.

Хакерское сообщество образовано достаточно разнородной совокупностью индивидов с широким спектром направлений противоправной деятельности, используемых методов и преследуемых целей.

Среди хакеров встречаются как любознательные подростки, так и опасные профессиональные преступники. На основании опроса 100 тыс. хакеров дается следующая приблизительная оценка распределения их по уровню квалификации: представители киберкриминала мирового класса – 0,1%; профессиональные хакеры – 9,9%; любители – 90,0%[11].

А.Л. Осипенко предлагает следующую типологию хакеров.

1. Многочисленная группа начинающих хакеров состоит из лиц, слабо разбирающихся в основах программирования и использующих готовые программные средства осуществления атак, зачастую даже не понимая принципов их действия. Для ее обозначения применяется термин "script kiddies". Таких любителей становится все больше, а наносимый ими ущерб превышает тот, который причиняют квалифицированные хакеры.

2. В основной группе хакеров нередко выделяют такие подгруппы, как "крэкеры" (субъекты, специализирующиеся на разрушении средств безопасности сетей или компьютерных систем с целью нелегального использования их ресурсов), "фрикеры" (лица, проникающие в телефонные сети и иные защищенные телекоммуникационные системы). В целом представители типичной группы хакеров имеют неплохие навыки программирования, способны создавать собственное программное обеспечение для взлома, лучше понимают основы функционирования вычислительных систем, на которые осуществляют нападение. Как правило, такие хакеры преднамеренно участвуют в противоправных действиях, связанных с блокированием работы сетевых систем, хищениями номеров кредитных карт, мошенничеством.

3. "Кодировщики" (coders) осуществляют взломы программного обеспечения. Типичный "кодировщик" не продает краденый материал, а распространяет бесплатно через специализированные сайты. Однако не все из них столь бескорыстны, некоторые предлагают платные услуги по взлому программ.

4. Хакеры "старой гвардии" (old guard hackers) в основном имеют высокую профессиональную подготовку при отсутствии прямых преступных намерений. Такие лица с некоторым превосходством относятся к требованиям норм права, считая, что им в сетях дозволено практически все. Они руководствуются в основном исследовательскими интересами.

Достаточно интересным является вопрос о принципах существования хакерских групп. Наибольшее распространение получили хакерские группы, участники которых имеют опосредованные сетевым общением связи и не ведут совместной преступной деятельности. В основном в таких группах обмениваются опытом взлома и устранения его следов, оказывают друг другу моральную поддержку.

Реже встречаются группы с устойчивыми связями. Однако и в них, как правило, совместная деятельность носит случайный характер, отсутствует признанный лидер и распределение ролей, все участники равноправны. Такие группы могут выполнять оплачиваемые заказы на взлом определенных сетевых систем.

Также встречаются и хорошо организованные группы с определенной иерархической системой. По оценкам специалистов, лишь на территории Москвы действует не менее восьми подобных хакерских группировок, в том числе имеющих межнациональные и трансграничные связи.

Особое место в хакерском сообществе занимают warez-группы, специализирующиеся на взломе программного обеспечения. Известны более 10 крупных международных группировок, осуществляющих шумные публичные акции.

Одна из старейших групп DrinkOrDie до недавнего времени имела свой "официальный" сайт, где утверждалось, что ее основал москвич по кличке Deviator в 1993 г. В 1995 г. деятельность группы приобрела международную известность. Именно тогда входящие в нее хакеры распространили "пиратскую" версию операционной системы Windows 95 на две недели раньше ее официального выпуска. А пресечена деятельность группы была в 2002 г., когда ее лидера, ответственного, по утверждению следственных органов, за распространение в Интернете основной части "взломанного" программного обеспечения, приговорили к трем годам и восьми месяцам лишения свободы.

Как и во многих подобных группах, в DrinkOrDie существовало определенное разделение обязанностей. "Поставщики" (supplier), в число которых входили администраторы компьютерных сетей и студенты крупнейших американских университетов, доставали программы до их официального выхода, "кракеры" взламывали защиту, "курьеры" обеспечивали распространение "доработанных" программ. К 2000 г. DrinkOrDie превратилась в крупную международную организацию, имеющую представительства во многих странах мира и объединяющую большое число более мелких групп. По различным оценкам, в составе таких групп насчитывалось до полутора тысяч активных членов в 12 государствах. Лидеры организации проживали в США и Австралии. Участники групп, как правило, не получали доход от своей незаконной деятельности, в основном они стремились получить имидж "взломщика"-профессионала[12].

Типологизация личности компьютерного преступника возможна по различным основаниям. В.В. Лунев отмечает, что мотивационная сфера является центром внутренней структуры личности, интегрирующим ее активность[13]. Под мотивационной сферой личности понимается вся совокупность ее мотивов, которые формируются и развиваются в течение ее жизни"[14]. Нельзя забывать и о том, что характер побуждений нередко выступает обстоятельством, отягчающим или смягчающим ответственность.

Основываясь на анализе результатов зарубежных и отечественных исследований, можно констатировать, что наиболее характерными мотивами лиц, совершающих компьютерные преступления, можно считать: корыстные; хулиганские; политические; игровые, исследовательский интерес; потребность в самоутверждении; месть; мотивы, связанные с психическими отклонениями.

Необходимо отметить, что масштабы корыстных преступлений против собственности и объемы причиняемого ущерба от преступлений в сфере компьютерной информации год от года увеличиваются. Все чаще заявляют о себе, в частности, вымогатели, промышляющие в компьютерных сетях. Излюбленным методом преступной деятельности таких лиц является умышленное заражение вирусом компьютерных сетей с последующим навязыванием услуг по их восстановлению за денежное вознаграждение. При этом группа вымогателей может разделить свои обязанности: внедряют вирус одни лица, а восстанавливают сети другие лица.

Как показывает анализ, корыстный тип компьютерного преступника – это, как правило, лицо, достигшее 25-летия. Для компьютерных преступников младшего возраста характерно совершение преступлений бескорыстного характера, в основном из любопытства, с целью самоутверждения, ради удовольствия, игры.

Для другой группы компьютерных преступников доминирующими являются мотивы, связанные со стремлением к самоутверждению. Представители этой группы зачастую пытаются получить известность путем создания вредоносных программ. Для представителей этого типа характерны честолюбие, целеустремленность, решительность, стремление к лидерству. Они отличаются хорошей приспособляемостью, так как ориентируются в социальных нормах и требованиях, имеют социальный опыт и могут контролировать свое поведение.

Криминологи отмечают частое сочетание мотивов корысти и утверждения себя в жизни[15]. Учитывая возрастные особенности лиц, совершающих преступления исследуемой категории, такое сочетание представляется вполне закономерным.

Нередко взломы, особенно направленные на блокирование работы систем, связаны и с различного рода деструктивными мотивами. Очевидно, определенная часть молодежи пытается реализовать свои наклонности к вандализму в киберпространстве, где все представляется не настолько серьезным, как в реальной жизни, и при этом велика вероятность остаться безнаказанным. Между тем исследователи полагают, что даже те противоправные деяния, которые принято объяснять хулиганскими деструктивными побуждениями, на самом деле связаны со стремлением подтвердить себя в качестве социального и биологического существа, т. е. все с тем же мотивом утверждения, основанным на потребности ощущать себя источником изменений в окружающем мире[17].

Среди типов компьютерных преступников, для которых корыстные мотивы не являются ведущими, можно выделить игровой тип. Поведение этого типа преступников детерминируется потребностью к игре, риску, испытать острые ощущения, включиться в эмоционально возбуждающие ситуации. Для игрового типа компьютерных преступников характерно отсутствие серьезных познаний в области программирования и компьютерной техники. Данная категория преступников имеет, как правило, лишь некоторые пользовательские навыки работы с компьютером. Их действия направлены на уничтожение, блокирование, модификацию, копирование ничем не защищенной информации, создание вредоносных программ. К игровому типу часто относятся несовершеннолетние лица, главным образом школьники. Примечательно, что, по мнению специалистов, пик активности вредоносных программ обычно приходится на осень и на период после зимних праздников. Именно тогда заканчиваются каникулы, во время которых юные программисты получают возможность практиковаться в создании подобных программ.

Следующий мотивационный тип компьютерных преступников составляют лица, которые руководствуются соображениями мести. Этих людей нельзя подвести под общие рамки вирусописателей, так как у каждого из них своя мораль. Их не интересуют закон и беспокойство о том ущербе, который может понести пострадавший. У каждого из них есть своя персональная цель. Их задача – нанести максимальный урон.

Кроме указанных к числу потенциальных преступников можно отнести лиц, страдающих новым видом психических заболеваний – информационными болезнями, или компьютерными фобиями. Эта категория заболеваний связана с нарушениями информационного режима человека под воздействием внешних или внутренних дестабилизирующих факторов как врожденного, так и приобретенного свойства, которые вызываются информационным голодом, информационными перегрузками, неплановыми переключениями с одного информационного процесса на другой, информационным шумом и др.

В отдельных случаях исследователи предполагают даже наличие определенной психологической зависимости субъекта, выражающейся в навязчивой потребности осуществлять взломы компьютерных систем. В 1993 г. в Англии на судебном слушании было признано, что обвиняемый в сетевых проникновениях Бедворт страдает подобной зависимостью. Аналогичная потребность наблюдалась и у К. Митника, которого ФБР включило в список 10 наиболее опасных преступников США. Судья, выносивший приговор Митнику, объявил, что “видит определенную параллель между его пристрастием к взлому компьютерных сетей и влечением других людей к наркотикам”[18]. Сам Митник утверждал, что он мог бы стать миллионером, продавая полученные секретные сведения, однако не использовал эти возможности, а лишь “развлекался”, взламывая чужую защиту.

Итак, изучение особенностей лиц, совершающих преступления, является важным условием правильной организации борьбы с определенным видом преступной деятельности. Для преступлений в сфере информационных технологий изучение личности преступника приобретает особую актуальность, так как в данном случае речь идет о субъектах, которые до недавнего времени не попадали в поле зрения правоохранительных органов.

Типологизация личности компьютерного преступника может проводиться по различным основаниям (например, по особенностям мотивации, по уровню подготовленности, преступной специализации и т.д.). Такие сведения позволяют наиболее полно составить обобщенный криминологический портрет субъекта, совершающего подобные преступления.

Библиографический список

1. IBM Global Security Analysis // Computer World. 2012. № 11. P. 29-30.

2. Rogers M. A New Hacker Taxonomy. Winniper, 2011. 85 p.

3. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Перевод с английского / Д. Айков, К. Сейгер, У. Фонсторх. М.: Мир, 1999. 351 с.

4. Антонян Ю.М. Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев, В.Е. Эминов. М.: Юристъ, 2008. 335 с.: ил.

5. Зубков А. Кевин Митник вышел на свободу // Мир Internet. 2000. № 3. С. 48–49.

6. Кузнецов А. Пираты в Интернете // Полиция России. 2013. № 2. С. 27–29.

7. Ломов Б.Ф. Методологические и теоретические проблемы психологии. М.: Наука, 2005. 349 с.

8. Лунеев В.В. Мотивация преступного поведения. М.: Наука, 1999. 290 с.

9. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: Монография. М.: Норма, 2004. 432 с.

---

[1] Кузнецов А. Пираты в Интернете // Полиция России. 2013. № 2. С. 27.

[2] Кузнецов А. Пираты в Интернете // Полиция России. 2013. № 2. С. 28.

[3] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: Монография. М.: Норма, 2004. С. 170.

[4] Rogers M. A New Hacker Taxonomy. Winniper, 2011. P. 34.

[5] Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Перевод с англ. / Д. Айков, К. Сейгер, У. Фонсторх. М.: Мир, 1999. С. 90.

[6] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: Монография. М.: Норма, 2004. С. 149.

[7] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: Монография. М.: Норма, 2004. С. 151.

[8] Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Перевод с англ. / Д. Айков, К. Сейгер, У. Фонсторх. М.: Мир, 1999.С. 91.

[9] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: Монография. М.: Норма, 2004. С. 155.

[10] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: Монография. М.: Норма, 2004. С. 158.

[11] IBM Global Security Analysis // Computer World. 2012. № 11. P. 29.

[12] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: Монография. М.: Норма, 2004. С. 163.

[13] Лунеев В.В. Мотивация преступного поведения. М.: Наука, 1999. С. 107.

[14] Ломов Б.Ф. Методологические и теоретические проблемы психологии. М.: Наука, 2005. С. 204.

[15] Антонян Ю.М. Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев, В.Е. Эминов. М.: Юристъ, 2008. 335 с.: ил. С. 168.

[16] Антонян Ю.М. Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев, В.Е. Эминов. М.: Юристъ, 2008. 335 с.: ил. С. 168.

[17] Зубков А. Кевин Митник вышел на свободу // Мир Internet. 2000. № 3. С. 48.