УДК 343.9 **DOI: 10.34670/AR.2020.93.3.006**

Социально-криминологический портрет хакера: концептуальный образ

Пучков Олег Александрович

Доктор юридических наук,
профессор кафедры теории государства и права,
Уральский государственный юридический университет,
620137, Российская Федерация, Екатеринбург, ул. Комсомольская, 21;
e-mail: puchkov@mail.ru

Исследование выполнено при поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 18-29-16148 «Трансформация права в условиях развития цифровых технологий».

Аннотация

Статья посвящена социально-криминологической характеристике личности хакера как основного субъекта преступлений в информационной среде. На основании статистических и социально-психологических данных формулируется тезис о том, что в настоящее время выделяются новые характеристики социально-криминологического портрета хакера. В частности, криминологи предлагают новый подход к осмыслению сущности профессионализма хакера, его некоторых биосоциальных характеристик. Делается вывод о том, что несмотря на многообразие выделяемых в криминологии типов хакеров, в настоящее время отсутствует единый, концептуально целостный социально-криминологический портрет хакера. Указывается на то, что исследование, проведенное автором данной статьи, является дискуссионным и направлено в первую очередь на привлечение внимания научного сообщества к новой проблематике, связанной с криминологическим портретом хакера.

Для цитирования в научных исследованиях

Пучков О.А. Социально-криминологический портрет хакера: концептуальный образ // Вопросы российского и международного права. 2020. Том 10. № 3А. С. 60-71. DOI: 10.34670/AR.2020.93.3.006

Ключевые слова

Хакер, криминология, социально-криминологический портрет, информационная среда, компьютерные преступления.

Введение

В современную цифровую эпоху анализ криминологического портрета личности правонарушителя приобретает особое значение. В связи с тем, что правоведы, как правило, пытаются исследовать личность преступника-хакера применительно к специфике либо его деятельности, либо половозрастных характеристик, либо его физического типа, либо определенных мотивов, ускользают ключевые параметры исследования криминологического портрета хакера. Наблюдается все возрастающая тенденция классифицировать хакеров на «белых» и «черных», законопослушных и незаконопослушных, взламывающих компьютерные программы и создающих разрушительные вирусы из интереса либо из целей наживы, что приводит к тому, что исследователи пренебрегают тем, что неважно, какой хакер перед нами в их сложной иерархии, но в любом случае это лицо, совершившее преступное посягательство на разнообразные элементы цифровой среды.

В целях нашего исследования мы использовали общетеоретические методы – анализ, синтез, сравнение, позволяющие: 1) определить наиболее значимые элементы предмета исследования; 2) объединить их в единое целое (в нашем случае – в криминологический портрет хакера) путем сопоставления различных конкурирующих теорий, взглядов; 3) упорядочить существующее знание о предмете исследования, который сводится к концептуальному образу личности преступника-хакера. Метод формально-юридического анализа позволил определить границы исследуемых отношений в киберпространстве. Специально-научный метод междисциплинарного исследования (правовой, культурологический, социологический) позволил точнее определить предмет исследования и специфику его верификации.

Основная часть

Современная правовая действительность – это сложная самоорганизующаяся система, структурные элементы которой не всегда состоят в строгой субординации и зачастую меняются местами, определяя новые рычаги воздействия на общество, государство и личность. Это порождает вполне закономерное стремление законодателя «ввести» их в правовые рамки, т. е. наполнить одинаковым для всех субъектов права содержанием. К таким относительно новым и мощным рычагам воздействия относится хакерское движение, состоящее из специфических субкультур и в значительной степени разнящееся в ходе своей эволюции, но тем не менее тяготеющее к определенной унификации.

Криминологический портрет хакера изучен и описан в трудах О.С. Алавердова, С.В. Баринова, О.Ю. Введенской, Р.Р. Гайфутдинова, К.Н. Евдокимова, Е.П. Ищенко, Е.А. Маслаковой, Г.Т. Мегрелишвили, В.В. Полякова, Л.А. Попова, О.Б. Скородумовой и др.[1]

[1] См., например: Алавердов О.С. Криминологическая характеристика преступлений, совершаемых с использованием компьютерных технологий // Известия высших учебных заведений. Северо-Кавказский регион. Общественные науки. 2009. № 2. С. 89-91; Баринов С.В. Криминалистическая характеристика личности преступника, совершающего преступные нарушения неприкосновенности частной жизни в киберпространстве // Сибирские уголовно-процессуальные и криминалистические чтения. 2015. № 2. С. 111-117; Введенская О.Ю. Характеристика личности интернет-преступников // Вестник Краснодарского университета МВД России. 2015. № 4. С. 116-118; Гайфутдинов Р.Р. Типы компьютерных мошенников // Вестник экономики, права и социологии. 2017. № 2. С. 54-58; Евдокимов К.Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) // Сибирский юридический вестник. 2011. № 1. С. 86-90; Евдокимов К.Н. Структуры и состояние компьютерной преступности в Российской Федерации // Юридическая

Социолого-психологический аспект криминологического портрета хакера рассмотрен в трудах М.М. Акулич, Ю.М. Антоняна, М.А. Бабаковой, А.Ю. Лаговского, С.В. Масленченко, О.Б. Скородумовой, В.В. Степанова, В.Е. Эминова и др.[2]

Следует признать, что хакер как единичный представитель множества подобных может рассматриваться с точки зрения развития и влияния на него цифровых технологий, новых ценностей современного мира, права в целом и правовых технологий в частности, темпоральных переменных, собственной субкультуры и личностной матрицы. Все это в единстве и формирует, на наш взгляд, социально-криминологический портрет хакера. Портрет понимается нами не столько как изображение или описание групп людей, конкретного человека, сколько как воссоздание облика какой-либо человеческой индивидуальности, в котором вместе с внешним сходством запечатлевается духовный мир модели (отображаемого человека), в котором прослеживаются типические образы представителя эпохи, социальной группы, виртуального мора и правовой действительности [Советский энциклопедический словарь, 1979, 1054].

Исследователи социально-криминологического портрета личности хакера по-разному трактуют его содержание. Так, Е.Д. Жоров, П.В. Тепляшин полагают, что это «обнаружение всех возможных форм отражения личности преступника в реальной действительности», которое «обеспечивает возможность сформировать представление об его общих и частных особенностях, а затем совместно с иной криминалистически значимой информацией верно и точно определить направления и методы розыска, задержания и последующего изобличения лица, виновного в совершении преступления» [Жоров, Тепляшин, 2018, 69].

В.В. Поляков и Л.А. Попов обращают внимание на то, что криминалистическая характеристика имеет общие черты с уголовно-правовой характеристикой преступлений, но в ней употребляется термин «личность», а не «субъект преступления». Они полагают, что это не случайно. «Ведь помимо вопросов, связанных с возрастом, дееспособностью и профессией, значение имеет множество иных качеств, свойств и черт, вместе характеризующих человека как личность» [Поляков, Попов, 2018, 257]. Аналогичной точки зрения придерживаются Ю. Колесников и О.С. Алавердов, которые полагают, что от субъекта преступления в сфере компьютерной информации необходимо отличать личность преступника с его социально-психологическими и биологическими признаками, совершившего общественно опасное деяние,

наука и правоохранительная практика. 2016. № 1. С. 86-94; Ищенко Е.П. Виртуальный криминал. М.: Проспект, 2014; Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Среднерусский вестник общественных наук. 2014. № 2. С. 114-121; Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий // Вестник Томского государственного университета. 2007. № 299. С. 180-181; Поляков В.В., Попов Л.А. Особенности личности компьютерных преступников // Известия Алтайского государственного университета. Юридические науки. 2018. № 6. С. 256-259; Скородумова О.Б. Хакеры // Знание. Понимание. Умение. 2005. № 4. С. 159-161.

[2] См., например: Акулич М.М. Поведение личности в формирующемся информационном обществе // Общество и право. 2005. № 1. С. 78-82; Антонян Ю.М., Эминов В.Е. Преступление и наказание: криминолого-психологический анализ. М.: Норма, 2016; Лаговский А.Ю. и др. Составление психологического портрета преступника. М.: ВНИИ МВД России, 2000; Масленченко С.В. Анализ социальных ролей в субкультуре хакеров // Аналитика культурологии. 2008. № 1. URL: https://cyberleninka.ru/article/n/analiz-sotsialnyh-roley-v-subkulture-hakerov; Скородумова О.Б. Хакеры как феномен информационного пространства // Социологические исследования. 2004. № 2. С. 70-79; Степанов В.В., Бабакова М.А. Поисково-познавательная деятельность при расследовании преступлений, совершенных с использованием высоких технологий. М.: Юрлитинформ, 2014.

которое не охватывается конструкцией состава преступления [Алавердов, 2009, 89; Колесников, 2005, 13].

Е.П. Ищенко полагает, что «нарисовать портрет хакера так же трудно, как, скажем, портрет типичного вора. Хакеры в основном мужчины, многие с высшим, чаще всего техническим, образованием или студенты. Как правило, это люди замкнутые и на контакты по известным причинам идут с большой неохотой. В какой-то степени их можно сравнить с разведчиками: мало кто умеет так мастерски собирать и анализировать информацию. У хакеров свой язык, малопонятный непосвященным. Общаются они почти всегда через компьютер – чтобы не "светиться", и только на английском, с множеством сокращений и примесью дополнительных символов с клавиатуры компьютера» [Ищенко, 2014, 10].

Следует отметить, что хотя единой криминалистической классификации свойств личности компьютерного преступника до настоящего времени не выработано, можно выделить биологическую, социальную, психологическую.

Абстрагируясь от типологии хакеров, обратим внимание на общую криминологическую картину личности хакера, понимаемую прежде всего как лицо, способное как «взломать систему», так и починить ее, преследуя при этом определенную цель и обладая соответствующей мотивацией. С.В. Масленченко полагает, что слово «хакер» невозможно адекватно перевести на русский язык – в первую очередь в силу его двусмысленности. Английский глагол «to back» применительно именно к сфере компьютерных технологий может иметь противоположное значение, при этом особенно важно, что «оба эти действия предполагают общую основу: понимание того, как система устроена, способность оперировать громадными массивами программных данных, не случайно то, что многие системные операторы – бывшие хакеры (в первом, "ломательном" смысле)» [Масленченко, 2008, www].

Таким образом, независимо от того, какой перед нами хакер – «белый» с ореолом романтизации или «черный» – кракер, спамер и т. д., все они взаимодействуют друг с другом и, имея некоторые отличия в субкультуре, в большой мере демонстрируют носительство их общих черт. Это связано прежде всего с тем, что «основным инструментом деятельности как у "черных», так и у "белых" хакеров выступает вирус. Программы активности вирусописателей постоянно дополняются новыми идеями и их объективациями в виртуальном мире» [Там же]. Многие ученые подразделяют «черных» хакеров на разновидности в зависимости от цели взлома: на вандалов, «шутников», экспериментаторов, взломщиков и др., тем не менее отнеся к «черным» хакерам (кракерам), к примеру, экспериментаторов[3] [Там же]. Внимание акцентируется не на том, что это преступная деятельность, а на том, что «злонамеренности или стремления к выгоде здесь нет – чистое баловство, в более широкой перспективе весьма к тому же полезное: именно из таких "экспериментаторов" и вырастают со временем настоящие компьютерные специалисты и "белые хакеры"» [Там же]. Нам представляется, что такая позиция автора не вполне соответствует концептуальной характеристике преступлений в сфере компьютерной информации, содержащихся в главе 28 УК РФ, определяющей, что неправомерный доступ к охраняемой законом информации влечет, как правило, общественно опасные последствия в значительном размере (нарушение правил доступа к охраняемой законом информации, нарушение ее конфиденциальности, целостности).

[3] По мнению автора, это пытливая молодежь, осваивающая киберпространство, а также нормы человеческого общежития в виртуальном мире, с которыми она экспериментирует и намеренно делает «как нельзя», чтобы посмотреть, «что будет».

В ч. 3 ст. 273 УК РФ предусмотрена уголовная ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, повлекшее тяжкие последствия или создавшее угрозу их наступления. «При этом квалифицированный состав статьи охватывает неосторожное причинение тяжких последствий, за которые предусмотрено самое тяжкое из всех наказание – до семи лет лишения свободы» [Чебыкина, Молдаванов, 2014, 577]. Тем самым преступление, предусмотренное ч. 2 и 3 ст. 273 УК РФ, допустимо, с нашей точки зрения, считать преступлением с двойной формой вины, при которой умысел направлен на совершение противоправных действий, образующих объективную сторону, а неосторожность может проявляться в отношении тяжких последствий.

Компьютерным преступником можно стать и в результате «невинных» детских забав, а устоявшаяся практика водораздела между «белыми» и «черными» хакерами, романтизация первых (от художественных фильмов до издания специальных журналов) явно не способствуют борьбе с компьютерными преступлениями. К слову сказать, практически нигде не идет речь о субкультуре «белых» хакеров, но без них «черное» хакерство было бы невозможно.

Также противоречиво, по нашему мнению, утверждение О.Ю. Введенской, которая не отрицает, что компьютерные преступления совершают профессионалы (в сфере программирования, в сфере телекоммуникационных систем) и при этом делает неожиданный вывод: «Интернет-преступники в большинстве своем специальными познаниями не обладают, так как для совершения преступных действий они им, как правило, не нужны. Свойства сети Интернет им необходимы для реализации умысла на совершение “традиционных” преступлений» [Введенская, 2015, 117]. В итоге автор приходит к следующему выводу: «Таким образом, анализируя полученные в результате проведенного исследования сведения о личности интернет-преступников, возможно выделить среди них две типовые характеристики таких лиц – собственно компьютерных преступников, использующих свойства сети Интернет в качестве способа совершения преступления, и новую группу – “продвинутых” представителей традиционной преступности, использующих интернет-возможности в качестве средства реализации преступного умысла» [Там же]. Исследователь при этом не уточняет, какой уровень знаний в сфере компьютерных технологий необходим для первой группы (имеют ли эти лица определенные профессии). Что же касается термина «продвинутые представители традиционной преступности, использующие интернет-возможности в качестве средства реализации преднамеренного умысла», то здесь хакерский сленг вряд ли внесет ясность. Речь, разумеется, должна вестись о профессионализме, который, по нашему мнению, возможен в первом случае и необходим во втором. Отметим, что некоторые русские правоведы (С.В. Познышев, И.Я. Фойницкий) выступали против употребления термина «профессиональный», но большинство ученых признавали необходимость этого термина. «В целом же терминология в отношении профессиональных преступников не была выдержана – их называли “привычными”, “упорными”, “хроническими”, “неисправимыми”» [Кузнецова, Лунеев, 2005, 488]. Некоторые исследователи связывали профессиональную преступность с особым родом деятельности и т. д.

Что же лежит в основе «продвинутости»? В чем заключается существенная разница между собственно компьютерными преступниками и «продвинутыми» представителями традиционной преступности?

Как известно, «профессиональный преступник» был выделен в классификации

преступников в 1897 г. на Гейдельбергском съезде Международного союза криминалистов. Как пишут Л.В. Тихомирова и М.Ю. Тихомиров, «это понятие связывалось с использованием определенных навыков в своем преступном промысле» [Тихомирова, Тихомиров, 2007, 719].

Профессиональная преступность – это по-прежнему методологическая проблема в криминологии. Заключается она, на наш взгляд, в том, что современное понимание профессии не всегда помогает в определении специфики компьютерных преступлений. В современной криминологии профессия понимается прежде всего как род занятий, требующий определенной подготовки, являющийся источником существования и одобряемый в социальном плане.

В криминологии относительно к совершаемым компьютерным преступлениям употребление термина «профессионализм» не всегда описывает профессионала с точки зрения полученного им образования. В учебнике «Криминология» для обозначения столь специфической преступной деятельности был введен в оборот термин «криминальный профессионализм». Речь идет не о преступной профессии, а о *проявлении ее объективных свойств в действиях субъекта*. Таким образом, данное понятие содержит четыре признака:

– устойчивость преступного занятия (специализация);

– определенные знания и навыки (квалификация);

– преступление как источник средств существования;

– связь с антиобщественной средой [Кузнецова, Лунеев, 2005, 492].

Такой подход в целом согласуется с нашим пониманием профессионализма в сфере компьютерных преступлений. В то же время он, по нашему мнению, не ставит никакого водораздела между более или менее профессиональными преступниками. Ведь для осуществления преступной деятельности в *сфере цифровых технологий* вовсе не обязательно иметь высшее образование программиста, достаточно овладеть определенными навыками, которые тоже будут свидетельствовать о «криминальном профессионализме»[4]. В любом случае навык, который принято отождествлять с автоматизмом в действии, всегда первоначально связан со всяким новым способом действия. «…Протекая первоначально как некоторое самостоятельное, развернутое и сознательное действие, затем в результате многократных повторений может осуществляться уже в качестве автоматически выполняемого компонента действия» [Ильичев и др., 1983, 393]. В связи с этим мы не можем согласиться с авторами «Философского энциклопедического словаря», утверждающими, что «навык не связан с устойчивой тенденцией к актуализации» [Там же]. Меняется технология виртуального мира, меняются и навыки, как это происходит, к примеру, у современных «спамеров». Следует согласиться с мнением С.В. Масленченко, согласно которому сложность анализа технологической ситуации в виртуальном мире заключается в том, что «информационная среда растет настолько большими темпами, что наука не только не может полностью контролировать эту технологическую ситуацию, она даже не успевает анализировать последствия этих трансформаций» [Масленченко, 2008, www].

Также следует обратить внимание на то, что зачастую исследователи криминалистического портрета хакера связывают его профессионализм или непрофессионализм с абсолютно непригодными для этого понятиями. Так, С.В. Масленченко, в ходе своего методологически выверенного исследования делает неожиданный вывод о том, что «*низменность мотивов*

[4] Навык понимается нами как умение в совершенстве выполнять целенаправленные действия, приводящие к решению определённых задач.

кракеров[5] и отсутствие стремления к профессиональному росту приводят к тому, что 90% из них являются кракерами-чайниками…» [Там же]. Каким образом автор усмотрел взаимосвязь низменных мотивов с отсутствием стремления к криминальному профессионализму? Какие критерии при этом применил?

Таким образом, даже те некоторые проблемы, обнаруженные нами при описании криминологического портрета хакера, приводят порой к значительным погрешностям. Обратимся к выводам некоторых исследователей в этой сфере. При этом отметим, что как бы ни разнились эти выводы, структура криминологического портрета хакера неизменна (социальные, психологические, биологические характеристики личности).

Следует согласиться с Н.В. Олиндер, что в современном мире происходит технологизация преступлений и «старые» преступления получают новое наполнение и трансформируются иногда настолько, что криминалистическая характеристика, разработанная ранее, перестает выполнять свое предназначение [Олиндер, 2016, 50]. Следовательно, личность преступника в современном цифровом мире тоже претерпевает изменения. Таким образом, личность хакера следует рассматривать также и на «срезе» технологических составляющих информационного поля, в котором хакер пребывает в момент совершения преступления. К примеру, Н.В. Олиндер предложила учитывать наличие закономерных особенностей при криминалистической характеристике компьютерных преступлений, совершенных с использованием электронных платежных средств и систем, которые, на ее взгляд, непосредственно влияют на личность хакера. Это «бездокументарный характер преступной деятельности, что порождает такое явление, как “виртуальный след”, удаленный доступ преступника к объектам системы электронных платежей, многообразие и сложность компьютерных программ, автоматизирующих осуществление расчетов, доступность компьютерных и платежных систем» [Там же, 51].

Правоведы, исследующие проблематику криминологического портрета хакера, зачастую связывают его с определенным видом преступления. Так, С.В. Баринов, исследуя криминалистическую характеристику личности преступника, совершающего преступные нарушения неприкосновенности частной жизни в киберпространстве, приводит следующие показатели: в 78% случаев преступники, совершившие такие преступления, – это мужчины, из которых 79% – лица в возрасте до 35 лет. Преступное посягательство направлено в основном на женщин (62%), причем все они в возрасте до 35 лет. «Из приведенных данных становится очевидной корреляционная связь между возрастом преступников и их жертв, что объясняется, прежде всего, рядом психологических и биологических факторов. Именно в возрастной категории до 35 лет между полами происходит активно поиск партнеров, установление близких отношений. Такие процессы иногда сопряжены с неудачами, разочарованиями и переживаниями, которые служат основой для формирования преступного умысла» [Баринов, 2015, 113].

Когда же речь идет о криминологическом портрете хакера в целом, то наблюдаются попытки либо анализировать определенные возрастные группы, либо выяснить определенный мотив, цель или только биологические характеристики личности, осуществляющей неправомерные действия в сети Интернет. К примеру, М.М. Акулич полагает, что хакерством занимаются молодые люди в возрасте 14-18 лет (иногда с 12 лет). Основными мотивами приобщения к хакерству являются «любопытство, а затем желание разобраться в сложной

[5] Курсив мой. – О.П.

технической задаче и решить ее; получение выгоды в форме различного рода компьютерных (дорогостоящих в российских условиях) программ. Получение же собственной денежной выгоды характерно лишь для хакеров-взломщиков или профессионалов, которые среди подростков возможны крайне редко» [Акулич, 2005, 81].

Основываясь на классификации возрастных групп компьютерных преступников, осуществленной на Первой международной конференции Интерпола по компьютерной преступности, проведенной в апреле 1995 г., лиц, совершающих компьютерные преступления, по-прежнему подразделяют на три группы: 11-15 лет, 17-25 лет и 30-45 лет [Комиссаров, 1995]. Но при этом следует учитывать, что от первого случая злоупотребления с использованием компьютера, зарегистрированного в 1958 г., и от первого преступления с использованием компьютера в бывшем СССР в 1979 г. в Вильнюсе прошла целая цифровая эпоха. Мир стоит на пороге новой биоцифровой революции, и остается только предполагать, каковы будут возрастные характеристики преступников.

Биологический элемент криминологического портрета хакера тоже имеет разную оценку исследователей. Как известно, определенные физические черты индивида могут предопределять его противоправное поведение, в том числе и при совершении компьютерных преступлений. Основоположниками «биологического» подхода к определению личности преступника являются Ч. Ламброзо, З. Фрейд, У. Шелдон и Э. Глюк. Ими была предпринята удачная попытка установить связь между предрасположенностью к преступной деятельности и строением тела человека.

К.Н. Евдокимов совершенно обоснованно полагает, что «физически слабый “хакер” вряд ли ввяжется в драку или пойдет на совершение насильственного преступления. С другой стороны, человек с низким уровнем интеллектуального развития, но хорошо развитый физически, вряд ли станет “хакером”» [Евдокимов, 2011, 86]. Он пишет: «Очень важна внешность хакера как наиболее яркая особенность его личности. “Хакер”, не обладающий привлекательными внешними данными или имеющий трудности общения со сверстниками, противоположным полом, ищет “самореализации” в “виртуальном мире”… он самоутверждается, пытаясь в интеллектуальной сфере возвыситься над сверстниками, увеличить в их глазах свою собственную личную значимость» [Там же].

Таким образом, свойства личности хакера складываются в значительной мере и под влиянием психофизиологических особенностей и его внешних данных. Так, В.В. Поляков и Л.А. Попов, ссылаясь на данные, полученные в ходе исследований многими учеными, приходят к выводу о том, что в современном криминологическом портрете типичного киберпреступника очень важны его внешние данные как лица, не обладающего привлекательностью и имеющего трудности общения. Они пишут, что в связи с распространением психических отклонений, связанных с фанатичным отношением к компьютерной технике и технологиям, зависимостями в их постоянном обновлении, повышении навыков в овладении новыми технологиями и т. д., формируются новые заболевания, которые теперь изучает так называемая информационная медицина [Поляков, Попов, 2018, 258].

Известно, что важнейшей особенностью российских хакеров (кардеров) является осуществление ими преступной деятельности в ночное время суток. Это объясняется режимом работы банковских и иных коммерческих структур в зарубежных государствах, а также специфической работой интернет-магазинов (круглосуточной). Ночная жизнь в виртуальном мире сказывается на физическом состоянии киберпреступников. Сбой биоритмов неизбежно приводит к серьезным заболеваниям. «Как отмечается исследователями, у таких лиц есть склонность к развитию интернет-зависимости; в СМИ также есть упоминания о болезни

киберпреступников Адриана Ламо и Райана Клири синдромом Аспергера – одной из форм аутизма, характеризующейся трудностями в социальном взаимодействии» [Гайфутдинов, 2017, 57]. В современной медицине появился новый раздел – информационные болезни, вызываемые нарушениями информационного режима: информационными перегрузками либо информационным голодом. Это еще больше усугубляет болезненное состояние личности, которое не может не проявиться во внешних данных киберпреступника.

Вместе с тем В.В. Поляков и Л.А. Попов приходят к выводу о том, что «несмотря на приведенные данные о типичном образе киберпреступников, мы полагаем, что он меняется. Представление о них как об инфантильных, субтильных, замкнутых, склонных к депрессиям, а также всевозможным злоупотреблениям, небрежно выглядящих молодых людях устарело. Сейчас быть киберпреступником модно прежде всего из-за того, что это выгодно в материальном плане. В результате в киберпреступность потянулись предприимчивые, авантюристичные и даже харизматичные люди, которые могут получить крупные преступные доходы, с большой вероятностью избежав при этом уголовной ответственности» [Полков, Попов, 2018, 257].

Социальные аспекты криминологического портрета хакера многообразны, но в целом их динамика за последнее десятилетие существенным образом не изменилась. Объем статьи не позволяет нам в полной мере осуществить анализ проблематики социальных черт криминологического портрета хакера, которые в настоящее время приобретают все большую значимость. Отметим лишь, что хакерский «вызов обществу» – это вызов обществом хакеров и даже придание им ореола борцов с несправедливостью и защитников отечества (вспомним атаки российских хакеров на зарубежные государственные сайты).

Приведем в качестве примеров, обобщающих все вышесказанное, некоторые варианты криминологического портрета современного хакера. «Изучение 62 приговоров по уголовным делам о неправомерном доступе к компьютерной информации, содержащихся в банке судебных решений РосПравосудия, позволило построить следующий среднестатистический криминалистический портрет личности компьютерного преступника, осуществляющего неправомерный доступ к компьютерной информации: лицо в возрасте от 17 до 26 лет, обучающееся в высшем учебном заведении либо являющееся техническим специалистом (например, программистом), ранее не имевшее судимости, являющееся жителем городской среды» [Жоров, Тепляшин, 2018, 70-71]. Аналогичной точки зрения придерживается К.Н. Евдокимов, полагающий, что даже неполнота анализа криминологического портрета личности компьютерного преступника позволяет сделать вывод о том, что «среднестатистический хакер – это студент или технический специалист (программист, системный администратор) в возрасте от 16 до 25 лет, ранее не судимый, постоянно проживающий в городских поселениях» [Евдокимов, 2011, 89].

С.В. Баринов полагает, что типичный портрет преступника, совершающего нарушения неприкосновенности частной жизни в киберпространстве, – «мужчина в возрасте от 17 до 35 лет, житель города, имеющий среднее специальное, незаконченное высшее или высшее образование, ранее не судимый, владеющий навыкам работы с персональным компьютером, активный пользователь сети Интернет, не женатый, психически неуравновешенный, испытывающий проблемы во взаимоотношениях с противоположным полом» [Баринов, 2015, 116].

О.Ю. Введенская полагает, что обобщенный портрет современного интернет-преступника выглядит следующим образом: «Интернет-преступления совершают как мужчины (65%), так и женщины (35%), в основном в возрасте 18-25 лет (60%) и 26-35 лет (40%), что позволяет сделать

вывод о сформировавшемся характере личности интернет-преступника; 40% имеют оконченное средне-специальное образование; 27% – студенты высших учебных заведений и 8% – студенты училищ, что говорит об их невысоком образовательном уровне, и лишь 25% имеют оконченное высшее образование; 62% интернет-преступников обладают посредственными, среднестатистическими навыками, работают в информационно-телекоммуникационных сетях, 36% обладают навыками "продвинутого" пользователя, вероятно, приобретенными самостоятельно, в отличие от компьютерных преступников, являющихся специалистами в рассматриваемой сфере, что необходимо для совершения преступлений. 56% интернет-преступников являются трудоспособными, но не работающими и не учащимися, 20% – учащимися, 10% – служащими, 6% – рабочими и только 10% среди них являются нетрудоспособными. При этом 45% довольствуются временными заработками, 33% являются работниками бюджетной сферы, и лишь у 22% деятельность связана с администрированием компьютерных сетей. 94% психических отклонений не имеют, что говорит об умышленном или спланированном характере совершаемых ими преступлений. 6% имеют психические отклонения, не исключающих вменяемость. Лиц, признанных невменяемыми, среди интернет-преступников нет» [Введенская, 2015, 117].

Заключение

Несмотря на объективную сложность концептуального описания социально-криминологического образа хакера, проведенное исследование свидетельствует о формировании в криминологической теории некоторых новых сущностных характеристик хакера как субъекта информационных преступлений. В этом смысле проведенное исследование является дискуссионным и направлено в первую очередь на привлечение внимания научного сообщества к новой проблематике, связанной с криминологическим портретом хакера.

Библиография

1. Акулич М.М. Поведение личности в формирующемся информационном обществе // Общество и право. 2005. № 1. С. 78-82.
2. Алавердов О.С. Криминологическая характеристика преступлений, совершаемых с использованием компьютерных технологий // Известия высших учебных заведений. Северо-Кавказский регион. Общественные науки. 2009. № 2. С. 89-91.
3. Баринов С.В. Криминалистическая характеристика личности преступника, совершающего преступные нарушения неприкосновенности частной жизни в киберпространстве // Сибирские уголовно-процессуальные и криминалистические чтения. 2015. № 2. С. 111-117.
4. Введенская О.Ю. Характеристика личности интернет-преступников // Вестник Краснодарского университета МВД России. 2015. № 4. С. 116-118.
5. Гайфутдинов Р.Р. Типы компьютерных мошенников // Вестник экономики, права и социологии. 2017. № 2. С. 54-58.
6. Евдокимов К.Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области)// Сибирский юридический вестник. 2011. № 1. С. 86-90.
7. Жоров Е.Д., Тепляшин П.В. Особенности криминалистической характеристики личности лица, совершающего неправомерный доступ к компьютерной информации // Эпоха науки. 2018. № 14. С. 68-71.
8. Ильичев Л.Ф. и др. (ред.) Философский энциклопедический словарь. М.: Советская энциклопедия, 1983. 839 с.
9. Ищенко Е.П. Виртуальный криминал. М.: Проспект, 2014. 228 с.
10. Колесников Ю. Внимание! Кибертерроризм! // Русский базар. 2005. № 38.
11. Комиссаров А.Ю. Первая международная конференция Интерпола по компьютерной преступности // Информационный бюллетень. 1995. № 14. С. 24-31.
12. Кузнецова Н.Ф., Лунеев В.В. (ред.) Криминология. М.: Волтерс Клувер, 2005. 629 с.
13. Масленченко С.В. Анализ социальных ролей в субкультуре хакеров // Аналитика культурологии. 2008. № 1. URL: https://cyberleninka.ru/article/n/analiz-sotsialnyh-roley-v-subkulture-hakerov

14. Олиндер Н.В. Преступления, совершаемые с использованием электронных платежных средств и систем: криминалистический аспект. М.: Русайнс, 2016. 120 с.
15. Поляков В.В., Попов Л.А. Особенности личности компьютерных преступников // Известия Алтайского государственного университета. Юридические науки. 2018. № 6. С. 256-259.
16. Советский энциклопедический словарь. М.: Советская энциклопедия, 1979.
17. Тихомирова Л.В., Тихомиров М.Ю. Юридическая энциклопедия. М., 2007. 972 с.
18. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24.05.1996: одобр. Советом Федерации Федер. Собр. Рос. Федерации 05.06.1996. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
19. Чебыкина К.Л., Молдаванов К.В. Развитие законодательства об ответственности за преступления в сфере компьютерной информации как направление правового обеспечения инновационных процессов в России // Молодой ученый. 2014. № 6. С. 575-578.

The socio-criminological profile of a hacker: the conceptual image

Oleg A. Puchkov

Doctor of Law,
Professor at the Department of theory of state and law,
Ural State Law University,
620137, 21 Komsomolskaya st., Ekaterinburg, Russian Federation;
e-mail: puchkov@mail.ru

Abstract

The article aims to identify the socio-criminological characteristic features of the personality of a hacker as the main subject of crimes committed in the information environment. The author of the article makes an attempt to carry out an analysis of scientific literature on the issue and the Criminal Code of the Russian Federation in order to reveal the characteristic features of the personality of hackers. In the modern digital age, the analysis of the criminological profile of a criminal is of particular importance. Taking into account statistical and socio-psychological data, the article points out that new characteristics of the socio-criminological profile of hackers are currently being identified. In particular, criminologists offer a new approach to understanding the essence of the professionalism of hackers and some of their biosocial characteristics, paying special attention to the reasons for their activities. The author concludes that despite the variety of types of hackers identified in criminology, there is currently no single, conceptually integral socio-criminological profile of a hacker. The article points out that the research that has been conducted provokes a lot of discussion and is aimed primarily at attracting the attention of the scientific community to new issues related to the criminological profile of a hacker.

For citation

Puchkov O.A. (2020) Sotsial'no-kriminologicheskii portret khakera: kontseptual'nyi obraz [The socio-criminological profile of a hacker: the conceptual image]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 10 (3A), pp. 60-71. DOI: 10.34670/AR.2020.93.3.006

Keywords

Hacker, criminology, socio-criminological profile, information environment, computer crimes.

References

1. Akulich M.M. (2005) Povedenie lichnosti v formiruyushchemsya informatsionnom obshchestve [The behaviour of individuals in the emerging information society]. *Obshchestvo i pravo* [Society and law], 1, pp. 78-82.
2. Alaverdov O.S. (2009) Kriminologicheskaya kharakteristika prestuplenii, sovershaemykh s ispol'zovaniem komp'yuternykh tekhnologii [Criminological characteristics of crimes committed with the use of computer technology]. *Izvestiya vysshikh uchebnykh zavedenii. Severo-Kavkazskii region. Obshchestvennye nauki* [Bulletin of higher education institutions. The North Caucasus region. Social sciences], 2, pp. 89-91.
3. Barinov S.V. (2015) Kriminalisticheskaya kharakteristika lichnosti prestupnika, sovershayushchego prestupnye narusheniya neprikosnovennosti chastnoi zhizni v kiberprostranstve [Forensic characteristics of the personality of a criminal who commits criminal violations of privacy in cyberspace]. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya* [Siberian criminal procedural and forensic readings], 2, pp. 111-117.
4. Chebykina K.L., Moldavanov K.V. (2014) Razvitie zakonodatel'stva ob otvetstvennosti za prestupleniya v sfere komp'yuternoi informatsii kak napravlenie pravovogo obespecheniya innovatsionnykh protsessov v Rossii [The development of legislation establishing liability for committing crimes in the field of computer information as a direction in legal support for innovation processes in Russia]. *Molodoi uchenyi* [Young scientist], 6, pp. 575-578.
5. Evdokimov K.N. (2011) Osobennosti lichnosti prestupnika, sovershayushchego nepravomernyi dostup k komp'yuternoi informatsii (na primere Irkutskoi oblasti) [The features of the personality of a criminal who gets unauthorised access to computer information (a case study of the Irkutsk region)]. *Sibirskii yuridicheskii vestnik* [Siberian law bulletin], 1, pp. 86-90.
6. Gaifutdinov R.R. (2017) Tipy komp'yuternykh moshennikov [Types of computer swindlers]. *Vestnik ekonomiki, prava i sotsiologii* [Bulletin of economics, law and sociology], 2, pp. 54-58.
7. Il'ichev L.F. et al. (eds.) (1983) *Filosofskii entsiklopedicheskii slovar'* [Encyclopedic dictionary of philosophy]. Moscow: Sovetskaya entsiklopediya Publ.
8. Ishchenko E.P. (2014) *Virtual'nyi kriminal* [Virtual crime]. Moscow: Prospekt Publ.
9. Kolesnikov Yu. (2005) Vnimanie! Kiberterrorizm! [Beware! Cyberterrorism!] *Russkii bazar* [Russian bazaar], 38.
10. Komissarov A.Yu. (1995) Pervaya mezhdunarodnaya konferentsiya Interpola po komp'yuternoi prestupnosti [The First international Interpol conference on computer crime]. *Informatsionnyi byulleten'* [Information bulletin], 14, pp. 24-31.
11. Kuznetsova N.F., Luneev V.V. (eds.) (2005) *Kriminologiya* [Criminology]. Moscow: Volters Kluver Publ.
12. Maslenchenko S.V. (2008) Analiz sotsial'nykh rolei v subkul'ture khakerov [Analysis of social roles in the hacker subculture]. *Analitika kul'turologii* [Analytics of cultural studies], 1. Available at: https://cyberleninka.ru/article/n/analiz-sotsialnyh-roley-v-subkulture-hakerov [Accessed 17/03/20].
13. Olinder N.V. (2016) *Prestupleniya, sovershaemye s ispol'zovaniem elektronnykh platezhnykh sredstv i sistem: kriminalisticheskii aspect* [Crimes committed with the use of electronic payment instruments and systems: the forensic aspect]. Moscow: Rusains Publ.
14. Polyakov V.V., Popov L.A. (2018) Osobennosti lichnosti komp'yuternykh prestupnikov [The features of the personality of computer criminals]. *Izvestiya Altaiskogo gosudarstvennogo universiteta. Yuridicheskie nauki* [Proceedings of the Altai State University. Legal sciences], 6, pp. 256-259.
15. *Sovetskii entsiklopedicheskii slovar'* [Soviet encyclopedic dictionary] (1979). Moscow: Sovetskaya entsiklopediya Publ.
16. Tikhomirova L.V., Tikhomirov M.Yu. (2007) *Yuridicheskaya entsiklopediya* [Legal encyclopaedia]. Moscow.
17. *Ugolovnyi kodeks Rossiiskoi Federatsii: feder. zakon Ros. Federatsii ot 13.06.1996 № 63-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 24.05.1996: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 05.06.1996* [Criminal Code of the Russian Federation: Federal Law of the Russian Federation No. 63-FZ of June 13, 1996]. Available at: http://www.consultant.ru/document/cons_doc_LAW_10699/ [Accessed 17/03/20].
18. Vvedenskaya O.Yu. (2015) Kharakteristika lichnosti internet-prestupnikov [The characteristics of the personality of Internet criminals]. *Vestnik Krasnodarskogo universiteta MVD Rossii* [Bulletin of Krasnodar University of the Ministry of Internal Affairs of the Russian Federation], 4, pp. 116-118.
19. Zhorov E.D., Teplyashin P.V. (2018) Osobennosti kriminalisticheskoi kharakteristiki lichnosti litsa, sovershayushchego nepravomernyi dostup k komp'yuternoi informatsii [The features of criminalistic characteristics of people who getting illegal access to computer information]. *Epokha nauki* [The epoch of science], 14, pp. 68-71.