УДК 343.91 № 4 (7) / 2015, с. 56-61

КРИМИНОЛОГИЧЕСКИЙ ПОРТРЕТ ЛИЦ, СОВЕРШАЮЩИХ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Ю. А. Мерзлов
Южно-Уральский государственный университет (национальный исследовательский университет), г. Челябинск, Российская Федерация

В статье рассматривается криминологическая характеристика лиц, совершающих преступления, предусмотренные главой 28 УК РФ. Представлен анализ их личности с позиции комплекса социально-демографических, уголовно-правовых, нравственно-психологических признаков.

Ключевые слова: преступность, личность преступника, компьютерные преступления, противодействие преступности.

CRIMINOLOGICAL PORTRAIT OF INDIVIDUALS COMMITTING COMPUTER CRIMES

Yu. Merzlov
South Ural State University (National Research University), Cheliabinsk, Russian Federation

The article discusses the criminological characteristics of individuals committing crimes under Chapter 28 of the Criminal Code of the Russian Federation. The analysis of their personality is presented from the perspective of socio-demographic, criminal-and-legal and moral-and-psychological characteristics.

Keywords: crime, offender's identity, computer crimes, combating crime.

Успех деятельности по предупреждению преступности возможен только в том случае, если определенный акцент будет направлен на выявление специфических черт личности преступника. Именно преступник является носителем причин совершенного преступления, «...основным и важнейшим звеном всего механизма преступного поведения» [8, с. 79].

Основные черты криминологической характеристики преступника представляют собой систему признаков, которые в совокупности характеризуют лицо, совершающее преступление. В литературе высказаны различные мнения о структуре основных черт криминологической характеристики личности преступника [2, с. 110-112; 6, с. 43-45], однако большинство авторов сходятся во мнении, что признаками личности преступника являются социально-демографические, уголовно-правовые и нравственно-психологические качества. В частности, В.Н. Кудрявцев предлагает наиболее полноценную по своему содержанию структуру личности правонарушителя:

социально-демографическая и правовая характеристика, которая охватывает пол, возраст, образование, семейное положение, профессию, социальное положение, характер совершенного правонарушения и прежнюю судимость;

нравственно-психологическая характеристика, включающая социальную и антисоциальную направленность личности, систему ценностных ориентаций, основные потребности и интересы, отношение к нормам морали, уровень правосознания;

основные психические и психофизиологические особенности;

социальное поведение, заключающееся в отношениях в производственном коллективе, семье, учебном заведении, ближайшем окружении, а также в связях с антиобщественными элементами и в самооценке [9, с. 188].

Полагаем, что такая структура личности в процессе изучения лиц, совершивших преступления в сфере компьютерной информации, на наш взгляд, является предпочтительной.

Компьютерная информация обладает целым комплексом отличительных свойств и признаков. В связи с этим необходимо сразу же обратить внимание на тот факт, что лицо, совершающее преступление в сфере компьютерной информации, обладает определенной совокупностью знаний, умений и навыков обращения с компьютером, программным обеспечением, компьютерными системами и сетями. С учетом данного тезиса важно подметить то, что навыки в общении с компьютерной техникой может в настоящее время приобрести практически каждый. Однако в зависимости от типа компьютерной информации (открытой, ограниченной либо конфиденциальной) доступ к ней может быть предоставлен различному по широте охвата кругу субъектов. Если доступ к открытой информации рассчитан на любого пользователя, то ограниченную либо конфиденциальную информация может получить только тот, кто знает соответствующие пароли, шифры, криптографические ключи, обеспечивающие защиту самой информации.

Наличие у индивида специальных знаний и навыков уже предполагает возможность совершения им действий, направленных на преодоление защитных механизмов на пути к получению информации. В то же время, лицо, совершающее компьютерное преступление, обладает специальными, глубокими по уровню знаниями, прочными навыками, позволяющими ему искать пути вскрытия ограниченной или конфиденциальной информации, раскрывая секреты ее защиты.

Исследование показывает, что представление характерологических особенностей личности преступника, совершающего противоправные посягательства в сфере компьютерной информации, целесообразно осуществить через типологию соответствующих лиц, применительно к тому или иному виду преступного деяния, определенного ст. 272-274 Уголовного кодекса РФ.

Оценивая удельный вес этих преступлений в структуре противоправных деяний в сфере компьютерной информации, необходимо указать, что доля неправомерного доступа к компьютерной информации составляет три четверти от всех деяний данного вида. Доля преступлений, заключающихся в распространении вредоносных программ для электронно-вычислительной техники, составляет 22% от общей численности компьютерных преступлений. Распространение носителей, содержащих вредные программы, совершается преимущественно при реализации пиратского программного обеспечения. Остальные 3% приходится на долю нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Предпосылками такого факта являются следующие объективные и субъективные обстоятельства:

широкое развитие сферы высоких технологий и значительная распространенность компьютерной техники среди населения;

наличие специальностей в высших образовательных учреждениях, по которым ведется подготовка обучающихся с привитием им профессиональных знаний, умений и навыков программирования;

влияние семейного и внесемейного окружения на процесс становления личности правонарушителя в сфере компьютерной информации;

фактическая безнаказанность лиц, совершивших компьютерные преступления, из-за высокой латентности данных противоправных деяний, отсутствие надлежащей подготовки сотрудников правоохранительных органов, осуществляющих производство по уголовным делам данной категории преступлений.

В литературе выделяются различные группы компьютерных преступников. Наиболее многочисленными среди них являются так называемые «хакеры» и «кракеры». Фактически и те и другие занимаются поиском уязвимых мест в вычислительных системах и осуществлением атак на данные системы [5, с. 49]. Однако основная задача хакера состоит в том, чтобы, исследуя вычислительную систему, обнаружить слабые места в ее системе безопасности и информировать пользователей и разработчиков системы с целью последующего устранения найденных недостатков, внести предложения по ее усовершенствованию [10, с. 11]. Вообще же, слово «хакер», согласно специальным источникам, обозначает талантливого законопослушного программиста [1, с. 91]. В какой-то степени с этим можно согласиться, так как в любом деле высоко оценивается профессионализм. Действительно, тот же системный администратор (даже если в системе всего два-три компьютера) обязан детально изучить операционные системы, особенности языков программирования и тонкости прикладных пакетов. Тем самым он, прежде всего, выявляет слабые и сильные стороны

компьютерных систем и использует полученные знания. Эти знания позволяют не только «защищать» системы от взлома, но и наоборот – «ломать» их. Таким образом, термин «хакер» совмещает в себе, по крайней мере, два значения: с одной стороны, это взломщик, а с другой – асс, мастер.

С точки зрения психофизиологических характеристик – это, как правило, творческая личность, способная идти на технический вызов, риск. В настоящее время крупные компании стремятся привлечь наиболее опытных хакеров на работу с целью создания систем защиты информации и компьютерных систем.

Кракер же, осуществляя взлом компьютерной системы, действует с целью получения несанкционированного доступа к чужой информации. Мотивы этого могут быть различными: от озорства до промышленного шпионажа.

Среди субъектов неправомерного доступа к компьютерной информации в зависимости от вида их деятельности выделяют еще:

фрикеров – людей, специализирующихся на использовании телефонных систем с целью уклонения от оплаты телекоммуникационных услуг;

кардеров, оплачивающих свои расходы с чужих кредитных карточек;

коллекционеров, использующих компьютерные программные продукты, перехватывающих различные пароли, а также коды телефонного вызова и номера телефонных компаний, имеющих выход к компьютерным сетям общего использования, например, Интернет;

киберворонов – злоумышленников, которые специализируются на несанкционированном проникновении в компьютерные системы финансовых, банковских расчетов. Обычно они используют компьютерные технологии для получения номеров кредитных карточек и другой ценной информации с целью наживы. Нередко полученную информацию они продают другим лицам;

компьютерных пиратов, специализирующихся на незаконном взломе систем защиты лицензионных компьютерных программных продуктов, которые потом распространяют за деньги по ценам, которые значительно ниже цен законных изготовителей.

Анализ публикаций отечественных и зарубежных авторов, касающихся проблемы характеристики личности компьютерного преступника свидетельствует о том, что криминолого-психологический портрет того же хакера, как правило, весьма абстрактен. В частности, указывается, что он рано знакомится с компьютером, компьютерная система и соответствующие технологии для него – смысл жизни, он социальный отщепенец, не обращающий внимания на окружающий мир, часто закомплексован, для большинства хакерство является первым настоящим достижением в реализации своих творческих начал и т. д. [4, с. 35; 11, с. 79; 14, с. 22].

Исследование показывает, что возрастной диапазон компьютерных правонарушителей колеблется в пределах от 14 до 45 лет. 54% преступников – это лица в возрасте от 18 до 25 лет; 13% – от 26 до 40 лет. Таким образом, свыше 75% выявленных преступников составляет молодежь и есть основания для опровержения многих устоявшихся в обществе стереотипах о возрастных особенностях личности хакера.

Преступления в сфере компьютерной информации мужчинами совершаются в 5 раз чаще, нежели лицами женского пола. Большинство субъектов таких преступлений имеют высшее или неоконченное высшее техническое образование (54%), а также другое высшее либо неоконченное высшее образование (19%). Однако в последние несколько лет наметилась отчетливая тенденция к увеличению доли женщин в структуре компьютерных преступников. Во многом это обусловлено профессиональной ориентацией некоторых специальностей и должностей, оборудованных автоматизированными компьютерными рабочими местами, которые чаще занимают женщины.

По нашим данным, полученным в ходе проведения соответствующего исследования, 52% правонарушителей имели специальную подготовку в области автоматизированной компьютерной обработки информации; 97% являлись сотрудниками государственных учреждений и организаций, которые использовали компьютерные системы и информационные технологии в своей повседневной деятельности, причем 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники.

На сегодняшний день имеют место факты совершения компьютерных преступлений и сотрудниками, занимающими в организации ответственные посты. Так, каждое четвертое из компьютерных преступлений совершаются руководителями организаций.

Современные руководители, как правило, специалисты высокого уровня, владеют достаточной компьютерной подготовкой и профессиональными знаниями, имеют доступ к информации широкого круга и могут отдавать распоряжения, хотя непосредственно за работу компьютерной системы не отвечают.

Следует иметь в виду, что в совершение компьютерных преступлений в нынешний период времени втянут широкий круг лиц, среди которых есть как дилетанты, так и высококвалифицированные специалисты. При этом все они имеют разный социальный статус и уровень образования, что уже позволяет всех их классифицировать на две большие группы – это как лица, состоящие с потерпевшим в трудовых или иных служебных отношениях, так и лица, не связанные с потерпевшим соответствующими деловыми контактами. К первой группе следует отнести сотрудников, которые злоупотребляют своим положением. Это различного рода клерки, работники службы безопасности, контролирующие работники, лица, занимающиеся организационными вопросами, инженерно-технический персонал. По данным проведенного исследования, доля программистов, инженеров, операторов и других работников организации, совершающих неправомерный доступ к компьютерным системам, составила 42%. Почти вдвое реже такой доступ совершается другими работниками (20%), а в 8% случаев такое правонарушение совершено бывшими работниками организации. Потенциальную угрозу составляют и представители других организаций, занимающихся сервисным обслуживанием и ремонтом систем. Во вторую группу входят лица, имеющие значительные познания в области компьютерных технологий и руководимые в большинстве случаев корыстными мотивами. К этой группе относятся также и специалисты-профессионалы, воспринимающие меры по обеспечению безопасности компьютерных систем как вызов своему профессионализму. Некоторые из них постепенно привыкают к ведению подобной деятельности и решают, что возможно совмещение материальных и интеллектуальных стимулов.

Практически каждый второй из числа лиц, относящихся к той или иной группе, – это все же дилетант, не обладающий глубокими познаниями в сфере компьютерных технологий, недостаточно уверенно владеющий навыками обращения с электронно-вычислительной техникой и компьютерными сетями.

Специалисты в области компьютерной безопасности считают, что наиболее многочисленны, но наименее опасны именно хакеры-дилетанты. На их долю приходится до 80% всех компьютерных атак. Но этих людей интересует не некая цель, а сам процесс атаки. Они испытывают удовольствие от преодоления систем защиты. Чаще всего их действия удается легко пресечь, поскольку хакеры-любители предпочитают не рисковать и не вступать в конфликт с законом [7, с. 132].

Большинство из лиц такого рода приобщились к компьютеру еще в школе. Знание компьютерных технологий ограничивается одним-двумя языками программирования. Наряду с хорошим уровнем технического образования или самообразования, общая образованность явно недостаточна (в текстах переписки «невооруженным» глазом виден «корявый» стиль и масса грамматических ошибок). Установка на преступное поведение среди дилетантов формируется стихийно, в основном под влиянием случайной цепи удачных и неудачных «взломов» защитных программ на других компьютерах. Закрепление такой установки происходит под влиянием «авторитетного мнения старших товарищей», высказанное ими после общения с «новичком» в сетевых «кулуарах».

С повышением уровня профессионализма, связанного с фактическим получением высшего технического образования, дилетанты приобретают более глубокие, систематизированные знания в области компьютерных технологий, языков программирования, прочные умения и навыки работы с сетями, программным обеспечением и т. д. Они уже являются специалистами. Психологически люди данной группы более уравновешенны, имеют отчетливо сформированную систему взглядов и ценностей, однако высокий уровень амбициозности им все же пока не присущ [3, с. 55-56]. В большинстве случаев, преступная «карьера» такого круга лиц трансформируется из «карьеры» любителя, либо складывается в результате вхождения в криминальную среду, например при содействии и протекции друзей-«профессионалов». Основной сферой преступной деятельности «специалистов» являются сетевой взлом, действия в операциях по получению кон-

фиденциальной информации, обладающей мощными системами защиты данных, промышленный и интеллектуальный шпионаж.

Наиболее опасную группу составляют все же профессиональные компьютерные преступники. Так, на долю этих лиц приходится порядка 80% всех преступлений, которые связаны с хищением материальных ценностей в особо крупных размерах с использованием компьютера. Лица этой группы характеризуются тем, что это высококвалифицированные специалисты с высшим юридическим, техническим или экономическим образованием. Они прекрасно разбираются в электронно-вычислительной технике, мастерски владеют программированием, их действия сопровождаются продуманной маскировкой поступков и сокрытием «следов» преступления. Знания этих людей в области компьютерных технологий обширны и глубоки: они владеют несколькими языками программирования, в совершенстве знают особенности аппаратной части современных компьютерных систем, имеют навыки профессиональной работы с несколькими компьютерными платформами, основными операционными системами и большинством пакетов прикладного программного обеспечения специализированного назначения, прекрасно информированы об основных системах электронных транзакций, системах сотовой связи, методах криптографии.

Психологически они уравновешенны, стойки к внешним воздействиям, крайне амбициозны, дальновидны, реально оценивают свои возможности, имеют связи с чиновниками из властных структур, которые нередко прибегают к их помощи для получения информации различного рода (в том числе и компрометирующей). Профессиональные компьютерные преступники работают в основном «для прикрытия» чаще всего руководителями подразделений информационных технологий в банках, иностранных компаниях, государственных учреждениях либо их заместителями, причем основная их деятельность связана с нелегальной и полулегальной деятельностью.

Для подавляющего большинства лиц, совершающих преступления в сфере компьютерной информации, характерны корыстные мотивы (67% лиц). Однако наряду и с корыстью выделяются и иные виды мотивов, определяющих соответствующее преступное поведение. В частности, мотивами рассматриваемой категории деяний являются политические мотивы (17%), так как глобальные компьютерные системы являются эффективным инструментом политических акций, мотивы мести (4%), озорство и хулиганские побуждения (5%), а также исследовательские интересы (7%), направленные для получения информации для собственных нужд или для осуществления соответствующей деятельности из-за мотивов самоутверждения.

Исследование мотивообразующих факторов, детерминирующих преступное поведение компьютерных преступников, свидетельствует о том, что все они могут быть сведены в три основные группы применительно к лицам, совершающим данные противоправные посягательства:

лица с ярко выраженным корыстным мотивом;

лица с отличительной особенностью устойчивого сочетания профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности [13, с. 82];

лица, страдающие новым видом психических заболеваний – информационными болезнями или компьютерными маниями [12, с. 59-60].

Если удельный вес первой группы лиц, чье поведение обусловлено жаждой наживы, составляет около 72%, то на долю второй и третьей групп приходится 24% и 4% соответственно.

Необходимо отметить, что правоохранительные органы, изучая природу рассматриваемых преступлений, осуществляют борьбу со злоумышленниками их же оружием – через Интернет. Преступность в сфере использования компьютерных технологий не признает границ, поэтому традиционные приемы обнаружения и борьбы с преступлениями данного вида пока недостаточно эффективны. В этом контексте актуальными являются комплексное исследование проблемы компьютерных преступлений, научный поиск эффективных путей повышения уровня информационной безопасности посредством совершенствования организационно-правовой защиты информации в компьютерных системах, решения проблем предупреждения компьютерных преступлений, подготовки специалистов-юристов в этой сфере, осуществляющих практику раскрытия и расследования соответствующих противоправных посягательств.

Примечания

1. Айков Д., Сейгер К., Фонстрох У. Компьютерные преступления. – М., 1999.
2. Алексеев А. И. Криминология. – М., 1999.
3. Бабаева Ю. Д., Войскунский А. Е. Психологические последствия информатизации // Психологический журнал. – 1998. – № 1. – С. 55-56.
4. Букин М., Букин Д. Хакеры. О тех, кто делает это // Рынок ценных бумаг. – 1997. – № 23.
5. Голубев В. Хакеры и кракеры: кто это? // Компьютерра. – 2002. – № 2.
6. Иншаков С. М. Криминология. – М., 2000. – С. 43-45.
7. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. – М., 2002. – С. 132.
8. Криминология. – М., 1995.
9. Кудрявцев В. Н. Причины правонарушений. – М., 1976.
10. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на INTERNET. – М., 2000. – С. 11.
11. Молчанов Б. М. Что такое хакер? // КомпьютерПресс. – 1993. – № 8.
12. Тихомиров О. К. Информационный век и теория Л.С. Выготского // Психологический журнал. – 2003. – № 1. – С. 59-60.
13. Тихомиров О. К., Гурьева Л. П. Психологический анализ трудовой деятельности, опосредствованной компьютерами // Психологический журнал. – 1996. – № 5. – С. 82.
14. Surgeon B. Хакеры // Компьютерра. – 1996. – № 43. – С. 22.

МЕРЗЛОВ Юрий Альбертович,
кандидат юридических наук, доцент, доцент кафедры уголовно-правовых дисциплин факультета Подготовки сотрудников правоохранительных органов, Южно-Уральский государственный университет (национальный исследовательский университет).
E-mail: mya2004@mail.ru

MERZLOV Yuriy,
Candidate of Law, Associate Professor, Chair of Criminal-and-Legal Subjects, Faculty of Law Enforcement Officers' Training, South Ural State University (National Research University).
E-mail: mya2004@mail.ru