

Баев Н.А.

Московский областной филиал
Московского университета МВД России имени В.Я. Кикотя (пос. Старотеряево)
Научный руководитель Е.Н. Гордеева

Криминологическая характеристика личности компьютерного преступника

Внедрение в управленческий процесс и другие сферы общества электронно-вычислительной техники является одним из достижений человека, без которого использование и обработка информации не представлялись бы возможными. Это повлияло и на развитие техники, отраслей знаний, принесло неопределимую пользу науке. Однако в преступных целях такие выгоды стали использоваться по мере развития научно-технического прогресса. Так, появились цифровые преступления, под которыми следует понимать общественно опасные виновные деяния, последствия от которых не идут в сравнение с ущербом от совершения иных противоправных действий уголовной направленности.

Актуальность исследований обусловлена резким приростом цифровой преступности в России. Целью исследования является рассмотрение характеристик личности компьютерного преступника, а также способов выявления лиц, совершающих преступления в сфере информационных технологий.

Непременным условием правильной организации борьбы с цифровыми преступлениями является осведомленность об особенностях лиц, совершающих такие преступления. Особую актуальность при раскрытии и расследовании преступлений определенного рода составляет познание личности, так как правоохранительным органам приходится в большинстве случаев сталкиваться с злоумышленниками, которые раньше не попадали в их поле зрения.

На сегодняшний день нельзя считать однородной группой совокупность лиц, совершающих компьютерные преступления, она по своему составу является разнородной. Стремление построить единообразный портрет информационных преступников изначально обречено на провал. Однако выявление характерных особенностей в той или иной мере обеспечивает расследование по уголовному делу.

Обычно среди молодежи это лица от 13 до 18 лет, которые, по их мнению, совершили грандиозное цифровое преступление, однако их способности не следует недооценивать. По отношению к объектам информационной безопасности к так называемым «группам риска» относятся: 1) уволенные из компании или временные сотрудники в организации, их персонал, которые могут или имеют доступ к вычислительной системе; 2) представители организованной преступности или конкурирующих структур; 3) лица, входящие в хакерские сообщества. Данные группы также могут пересекаться и варьироваться.

Е.В. Беляев¹ считает, что к личности компьютерного преступника относятся лица от 18 до 30 лет, которые из-за затруднений в межличностных отношениях приобрели комплекс неуверенности и неполноценности. К их особенным чертам автор относит ограниченность в общении. Такой человек склонен к анонимности, не любит оказываться на виду, на связь выходит посредством подключения при помощи модема. Коммуникация у таких лиц осуществляется в основном посредством телекоммуникационной сети Интернет. Обычно такие злоумышленники создают сообщества, в которых обмениваются опытом, мнениями и предпочтениями.

По мнению В.П. Талимончика², характеризующими чертами преступника, осуществляющего противоправную деятельность с использованием цифровых технологий, являются свободолюбие, высокий интеллектуальный уровень, подавленность эмоционального самовыражения. По его мнению, такие люди считают себя умнее и образованнее других, развлечениям предпочитают одиночество, чаще всего имеют комплексы, сочетают «гнусный цинизм» с восторженным романтизмом. Исследователь описывает компьютерного преступника как бодрствующего, проявляющего активность в ночное время суток. Компьютер для такого преступника является средством для самовыражения.

Сетевые преступления, согласно проведенному криминологами анализу материалов уголовных дел, совершаются гражданами от 14 до 25 лет, в 95% случаев лицами мужского пола.

Н.И. Селиванов, анализируя мотивацию преступников в области осуществления противоправной деятельности в сфере цифровых преступлений, определяет пять основных мотивов: 1) политические цели – 15%; 2) корыстные побуждения – 60%; 3) месть – 7%; 4) озорство и хулиганские побуждения – 3%; 5) исследовательский интерес – 15%. Также, по его мнению, мотивационная сфера преступной деятельности среди молодежи направлена на достижение конкретного социально-ролевого статуса или положения в хакерском сообществе и на повышение самооценки и приобретение признания со стороны значимого для того или иного лица окружения. Автор выделяет основные качества киберпреступника: прозорливость, хитрость, образованность, сообразительность, хвастовство и завышенная самооценка. Такие лица обычно презрительно относятся к людям, которые далеки от вычислительной техники³.

Несмотря на различные черты киберпреступников, отмечаемые авторами, исследователи-криминологи выделяют следующие причины соверше-

¹ Беляев Е.В. Типы личности «компьютерного преступника» // Законодательство и экономика. 2014. № 5. С.74-77.

² Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств // Законодательство и экономика. 2005. № 5. С. 57-62.

³ Селиванов Н.И. Проблемы борьбы с компьютерной преступностью // Законность. 2003. № 8. С. 37-41.

ния преступлений в области компьютерных технологий: 1) слабая изученность компьютерных преступлений с точки зрения криминологии; 2) постоянная модернизация и эволюция технических средств, а соответственно, и способов совершения преступлений в области цифровых технологий; 3) проявление большого интереса к изучению устройства и функционирования электронно-вычислительных машин со стороны молодежи, что может рассматриваться одновременно как позитивное и негативное явление; 4) недостаточность разработки теоретической модели преступлений в телекоммуникационной сфере.

К условиям, способствующим совершению цифровых преступлений, криминологи относят следующие: 1) чрезвычайно слабая регламентация отношений, которые возникают при применении и использовании информации и электронно-вычислительных устройств; 2) отсутствие норм в уголовном законодательстве, закрепляющих компьютерные преступления; 3) неготовность к борьбе с цифровой преступностью правоохранительных органов; 4) отсутствие обеспечивающих защиту компьютерной информации технических средств от воздействия преступных элементов; 5) полное или частичное отсутствие следовой информации о совершении преступления; 6) трудности, возникающие при установлении времени, места и способа совершения противоправного деяния.

Голубятников Д.А.

Московский областной филиал

Московского университета МВД России имени В.Я. Кикотя (пос. Старотеряево)

Научный руководитель Е.Н. Гордеева, кандидат педагогических наук

Основные детерминанты киберпреступности

В современном постиндустриальном обществе все большее значение приобретает использование информационных технологий, функционирование которых основано на принципах цифрового кодирования. Достижения научно-технологического прогресса внедряются во все сферы общественной жизни: дистанционная регистрация на общегосударственных и муниципальных информационных ресурсах, оплата коммунальных платежей, осуществление банковских операций, приобретение товаров и услуг, получение образования и т.д. Вполне естественно, что полноценное функционирование всех институтов общества невозможно без использования электронно-вычислительной техники, способной посредством серверного соединения подключаться к глобальной информационной сети Интернет. Все большее количество транснациональных корпораций и частных организаций дифференцируют рабочие места, требующие, соответственно, компетентных специалистов с техническим