ХАРАКТЕРИСТИКА ЛИЧНОСТИ ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Ю.С. Трушева, АлтГУ, юридический факультет, магистрант 1 к.
Научный руководитель – ***В.В. Поляков,*** к.ю.н., доцент.

Личность преступника всегда была одной из центральных проблем всех наук криминального профиля. Успешное предупреждение преступлений невозможно без изучения криминалистически значимых свойств личности преступника [1].

С распространением компьютерных технологий в повседневной жизни произошло увеличение количества преступных посягательств, совершенных с использованием электронно-вычислительной техники [2].

Компьютерное преступление и личность преступника сильно взаимосвязаны [3]. С точки зрения А.Б. Попова, компьютерных преступников можно разделить на три группы.

Первая группа - начинающие преступники. Чаще всего это выпускники (или студенты старших курсов) технических вузов, имеющие постоянный доступ к ЭВМ, вращающийся в сообществах, интересующихся компьютерными технологиями. Средний возраст – 15–20 лет. Пол – в подавляющем большинстве случаев мужской. Образование – среднее, среднее специальное или высшее, в некоторых случаях неоконченное. Происходят из семей среднего достатка. К компьютерной технике «приобщились» в большинстве случаев уже с 8–9 класса средней школы. Имеют дома один или более персональных компьютеров. Знание компьютерных технологий не ограничивается языками программирования низкого и высокого уровней и включает в себя знание аппаратной части выбранной платформы. Редко работают официально. Связь с внешним миром поддерживают в ограниченном объеме. Преимущественно имеют технического образование, гуманитарные знания не высоки (в письменной речи много грамматических ошибок). В разговоре употребляют особый компьютерный жаргон, сленг, смешивают русский и английский языки. Характеризуются несобранностью, небрежностью, практически постоянно читают литературу «по профессии».

Вторая группа – «закрепившиеся» преступники. Возраст 20–25 лет. Пол – в основном, мужской, но наблюдается тенденция к увеличению числа лиц женского пола (на сегодняшний день это около 5%). Образование – среднее, среднее специальное, высшее и незаконченное высшее, в основном – техническое. При совершении преступлений используют набор заранее подготовленных средств совершения преступлений, готовые решения, разработанные представителями первой группы преступников или другими членами своей группы. Часто являются организаторами хакерских атак с исполнителями из первой группы. В большинстве случаев лица, принадлежащие к этой группе, имеют постоянную работу в качестве технических консультантов и системных администраторов в фирмах, консультантов в компьютерных фирмах (что позволяет им в определенных случаях получать доступ к компьютеру жертвы, устанавливать вредоносное программное обеспечение для дальнейшего использования в преступных целях). Основная сфера «деятельности» – сетевой взлом, отдельные действия в операциях по получению защищенной информации.

Третья группа - профессионалы. Возраст 25–45 лет. Пол: мужской – 92%, женский – 8%. Социальное происхождение – семьи с достатком выше среднего. Образование – высшее техническое, возможно не одно. Имеются высокие знания в области компьютерных технологий: люди этой группы владеют несколькими языками программирования всех уровней, в совершенстве знают особенности аппаратной части современных компьютерных систем, имеют навыки профессиональной работы с несколькими компьютерными платформами. Психотип уравновешенный, стойкий к внешним воздействиям, с устоявшимися взглядами и системой ценностей. Личности амбициозные. Работают в основном «для прикрытия», например, начальниками отделов информационных технологий в крупных, в том числе иностранных, компаниях и государственных учреждениях. Основная же деятельность происходит в нелегальной и полулегальной сферах [4].

Н.Н. Федотов приводит следующее описание самых типичных образов компьютерных преступников. Стоит отметить, что наименование каждого типа дается автором условно.

Первый тип – «хакеры». Основной мотивацией хакеров являются исследовательский интерес, любопытство, стремление до-

казать свои возможности, честолюбие. Средства защиты компьютерной информации и ее недоступность они воспринимают как вызов своим способностям. Первой чертой личности «хакера» является эскапизм – бегство от действительности, стремление уйти от реальности, от общепринятых норм общественной жизни в мир иллюзий. «Хакер» имеет узкий круг общения и предпочитает всем другим контактам сетевые. Второй чертой данного типа личности является некриминальная направленность мыслей «хакера». Это, как правило, выливается в уделение малого внимания заметанию следов, непринятие мер конспирации. Часто у него даже отсутствует само осознание того факта, что совершается уголовное преступление.

Несколько более распространенным типом компьютерных преступников являются лица, не слишком хорошо владеющий знаниями в области информационных технологий, но зато владеющими доступом в информационную систему в силу служебного положения – так называемые «инсайдеры». Если для «внешнего» хакера обнаружить уязвимость в информационной системе представляет собой отдельную задачу, то для сотрудника организации почти все уязвимости видны с самого начала. Однако руководители и даже сотрудники службы безопасности, которым доверена такая информационная система, обычно излишне доверяют собственным сотрудникам.

Типичный «инсайдер» совершает компьютерное преступление (лично или в форме подстрекательства, совместно с «внешним» соучастником) с использованием сведений, полученных в силу служебного положения. Такими сведениями могут выступать пароли, знания о конфигурации информационной системы, знания о ее уязвимостях, о принятых процедурах. В ряде случаев этими сведениями «инсайдер» владеет «официально», то есть они ему необходимы для выполнения работы. Часто бывает, что реальный доступ сотрудников к конфиденциальной информации значительно шире, чем формальный или чем необходимый.

Следующий тип преступников совершают преступление из предприимчивых мотивов. Этот тип не является квалифицированным ИТ-специалистом и не имеет служебного положения, которым можно злоупотребить. С самого начала планирования преступления осознается его противозаконность. Решение совершить

преступление именно в компьютерной (сетевой) среде принимается не из-за своих особых знаний в этой области, а исключительно на основе рационального анализа, считая, что так будет выгоднее. Указанному типу преступников отвечает большинство кардеров, спамеров и фишеров.

Стоит отметить интернет-мошенников, которые руководствуются не только извлечением прибыли. Их преступный доход часто бывает меньше, чем средняя зарплата специалиста той же квалификации. Таких компьютерных преступников Н.Н. Федотов относит к «антисоциальному» типу. Мотивом для совершения мошенничества является антисоциальная психопатия (социопатия). Обычно такие типы действуют импульсивно и не склонны к планированию, особенно долгосрочному [5].

Таким образом, оценивая вероятного преступника, важнее всего установить его психотип и уровень технических знаний, а также мотив преступления.

Специфика преступлений, совершаемых в сфере компьютерных технологий, накладывает отпечаток на личность преступника, которая приобретает целый ряд особенностей [6]. Детальное изучение личностных характеристик преступников данной сферы может не только помочь выйти на след виновного, но и может способствовать профилактике данного вида преступлений среди так называемых групп риска.

Список литературы

1. Поляков В.В. Криминалистическая структура мер предупреждения компьютерных преступлений // Библиотека криминалиста: научный журнал. 2013. №5 (10). С. 287 - 291.
2. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – 247 с.
3. Попов А.Б. Криминологическая характеристика личности преступника, совершающего преступление, предусмотренное ст. 272 УК РФ // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2009. № 8. С. 411–413
4. Ковалев Д.И. Криминологическая характеристика преступника, совершающего преступление в сфере компьютерной информации // Вестник Академии. 2011. №3. С. 90-92

5. Федотов Н.Н. Форензика – компьютерная криминалистика. Москва: изд-во «Юридический Мир», 2007. С. 41-47.
6. Гавло В.К. Криминалистическая характеристика преступлений в сфере компьютерной информации / В.К. Гавло, В.В. Поляков // Право и государство: приоритеты XXI века: матер. Всерос. науч.-практ. конф. / под ред. В.Я. Музюкина, Е.С. Аничкина. – Барнаул: Изд-во Алт. ун-та, 2007. – С. 503 - 5