ОСОБЕННОСТИ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПОТЕРПЕВШИХ ПО КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ

Д.С. Шурыгина, Вит.В. Поляков
Алтайский государственный университет, г. Барнаул

Важную роль в раскрытии и предупреждении компьютерных преступлений имеет информация о личности потерпевших от них граждан и пострадавших организаций. Научное исследование данного вопроса осложняется крайне высокой латентностью данных преступлений. Для изучения реальной ситуации, включающей данные по невыявленным преступлениям большое значение оказывает разработка и проведение анкетных исследований различных категорий лиц, сталкивающихся с компьютерными преступлениями, а также разработка и использование современных информационных технологий, позволяющих на автоматизированном уровне собирать данные, входящие в криминалистическую характеристику компьютерных преступлений, например, с помощью технологии «Honeypot» [1].

Особенностью компьютерных преступлений является то, что об их совершении потерпевшие далеко не всегда вовремя или в принципе заявляют в правоохранительные органы. Более того, при обращении сотрудников следственных и оперативно-розыскных органов к ним для проверки сообщений о преступлении с их стороны может наблюдаться нежелание идти на сотрудничество, вплоть до попытки уклониться от дачи показаний или дать показания не соответствующие действительности [2]. Многие организации, особенно в кредитно-финансовой сфере, пострадавшие от компьютерных преступлений, стремятся скорейшим образом прекратить возбужденные уголовные дела, в том числе на основании примирения с преступниками. При этом примирение зачастую бывает притворным, когда в действительности вред не заглажен, либо заглажен символически [3]. Более того, некоторые потерпевшие активно противодействуют следствию, уничтожая следы совершенного преступления. Причиной указанного поведения потерпевших может являться страх перед тщательным расследованием, которое способно выявить всевозможные внутренние махинации и нарушения, либо спровоцировать вопрос о персональной ответственности или профессиональной непригодности руководителей или сотрудников организаций. По справедливому мнению И.М. Рассолова, для многих потерпевших

ущерб от преступлений зачастую кажется незначительным и несоразмерным проблемам, возникающим в связи с процедурой расследования, а также низкой вероятностью привлечения к ответственности виновных [4].

Исходя из анализа уголовных дел, связанных с неправомерным доступом к компьютерной информации можно прийти к следующим выводам о личности потерпевших: как правило, ими являются мужчины в 54,8% случаев, а женщины - в 45,2%. Средний возраст потерпевших составляет около 30 лет, что на 4 года меньше, чем в иных преступлениях. В 90,5% случаев потерпевшие не были знакомы с преступниками, что можно объяснить удаленным доступом к компьютерной информации за счет применения информационно-телекоммуникационных технологий, а также использованием специализированного вредоносного программного обеспечения, позволяющего преступникам отыскивать малозащищенные компьютеры, подключенные к сети Интернет [5].

Отметим, что от некоторых качеств потерпевших и их поведения нередко зависит совершение преступления, особенности его протекания и преступный результат. Легкомысленное, небрежное или халатное отношение к информационной безопасности с их стороны способствует совершению преступлений, выступая в качестве причины или благоприятных условий, при которых оно становится возможным, облегчая, либо провоцируя преступников на совершение преступлений в их отношении. Виктимные свойства личности проявляются в основном в несоблюдении или незнании элементарных правил информационной безопасности.

Чаще всего компьютерные преступления происходят из-за слабых знаний потерпевших о способах и средствах защиты компьютерной информации. Так, в 2014г. в г. Барнауле преступник с помощью принадлежащего ему компьютера получил учетную запись и пароль к электронному почтовому ящику, принадлежащему потерпевшей. Это позволило ему осуществить неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в электронном почтовом ящике, и дало возможность модифицировать охраняемую законом компьютерную информацию. В данном способе совершения преступления использовался прием, когда пароль был получен с помощью угадывания секретного вопроса, ответ на который был подобран достаточно просто и

быстро с помощью данных о жизни потерпевшей, которые было не сложно получить [6].

Достаточно часто в последнее время встречаются преступления, когда на почве ревности возникает преступный умысел, направленный на нарушение тайны телефонных переговоров и неправомерной доступ к охраняемой законом компьютерной информации, осуществляемые в отношении знакомых и родственников [7]. На основе анализа судебно-следственной практики, анкетирования сотрудников и специалистов в области информационной безопасности можно сделать выводы о типичных категориях потерпевших по компьютерным преступлениям. К их числу относятся как граждане, так и организации.

Абоненты сетей связи также достаточно часто становятся потерпевшими от компьютерных преступлений. Так, в г. Пенза, преступница, являясь специалистом офиса обслуживания и продаж одного из сотовых операторов связи, в рабочее время осуществляла неправомерный доступ к охраняемым законами персональным данным абонентов, которые копировала на принадлежащий ей мобильный телефон [8].

Потерпевшими по делам о фишинге являются пользователи, чьи конфиденциальные данные были получены мошенниками путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. Отметим, что порядка 95% преступлений данной категории являются латентными [9].

Потерпевшими по делам о преступлениях в сфере компьютерной информации нередко становятся владельцы и администраторы сайтов, когда происходит блокирование или замена содержимого веб страниц. Некоторые взломщики делают дефейс [10] сайта для получения признания в крэкерских кругах, повышения своей известности или для того, чтобы указать администратору сайта на его недостаточную защиту. Обычно потерпевший не заинтересован в разглашении информации об инциденте, поскольку, как уже говорилось ранее, это может нанести вред деловой репутации. Так, в Астраханской области преступник получил доступ к логину и паролю администратора сайта, а также блокировал указанный сайт в период с 19 часов 26 минут 17 ноября до утра 18 ноября 2015 г. (точное время не было установлено). Блокирование сайта повлекло невозможность в указанное время осуществлять

требуемые операции над компьютерной информацией и принесло вред деловой репутации [11], а также могло причинить прямой материальный ущерб и упущенную выгоду, о чем потерпевшим не заявлялось.

Во многих случаях, потерпевшим по преступлениям в сфере компьютерной информации являются крупные зарубежные компании-правообладатели. Не все они заинтересованы в уголовном преследовании виновных, зачастую стремясь только прекратить незаконное распространение защищаемого объекта, что причиняет им убытки. Так, в г. Орск преступник умышленно, исходя из корыстной заинтересованности, неправомерно приобрел через сеть Интернет контрафактные экземпляры программных продуктов, правообладателем которых является корпорация Microsoft и скопировал их на флэш-карту. Затем он стал незаконно хранить у себя указанные контрафактные экземпляры программных продуктов с целью последующего их сбыта за денежное вознаграждение посредством публичной оферты, размещенной на Интернет-сайте [12].

На сегодняшний день происходит множество преступлений в сфере компьютерной информации, однако лишь малая часть из них получает судебную перспективу из-за высокой латентности. В этой связи сложно выделить реальные признаки личности потерпевших в данных преступлениях, так как обобщение и анализ судебной практики не позволяет делать точные выводы, относящиеся к реальной ситуации. Это обстоятельство предполагает, что исследования в области потерпевших по компьютерным преступлениям необходимо продолжать.

Публикация подготовлена в рамках поддержанного РФФИ научного проекта 16-33-01160-ОГН.

Библиографический список

1. Лапин, С.А. Архитектура исследовательской Honeypot системы / С.А. Лапин, В.В. Поляков // Ломоносовские чтения на Алтае: Фундаментальные проблемы науки и образования: матер. Междунар. молодежной школы-семинара (Барнаул, 11-14 ноября 2014 г.). – Барнаул : Изд-во Алт. ун-та, 2014. – С. 821-824.
2. Анин, Б.Ю. Защита компьютерной информации. - СПб.: БХВ-Петербург, 2000. -384с.
3. Поляков, В.В. Деятельное раскаяние по делам о компьютерных преступлениях / В.В. Поляков // Современные

проблемы юридической науки : сб. науч. статей / под ред. Л.П. Чумаковой. – Новосибирск, 2011. – Вып. 9. – С. 156 - 159.
4. Рассолов, И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов. - М.: Норма, 2009. - 384 с.
5. Федоренко, В.И. Виктимологический аспект преступлений в сети Интернет. URL: https://zakon.ru/blog/2012/1/19/viktimologicheskij_aspekt_prestuplenij_v_seti_internet (дата обращения 10.06.17).
6. Поляков, В.В. Криминалистический анализ относительно простых способов совершения компьютерных преступлений / В.В. Поляков // Южно-уральские криминалистические чтения: Сборник докладов Всеросс. науч.-практ. конф. Вып. 24. – Уфа: РИЦ БашГУ, 2016. – С. 48-51.
7. Уголовное дело № 1-308/2016 по ст. ч.1 ст.138, ч.1 ст. 272 УК РФ) // Архив Московского районного суда г. Твери. 2016 г.
8. Уголовное дело № 1-316/2016 (по ч. 3 ст. 272 УК РФ) // Архив Железнодорожного районного суда г. Пензы. 2016 г.
9. Старичков, М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристика: автореф. дис. … канд. юрид. наук / М.В. Старичков. - Иркутск, 2006. – С. 3.
10. Дефейс // Википедия. URL: http://ru.wikipedia.org/?oldid=86406971 (дата обращения: 07.07.2017).
11. Уголовное дело № 1-178/2016 (по ст. ч.1 ст. 272, ч.1 ст. 273 УК РФ) // Архив Харабалинского районного суда Астраханской области. 2016 г.
12. Уголовное дело № 1-92/2017 (по ст. ч.2 ст.146, ч.2 ст. 272 УК РФ) // Архив Советского районного суда г. Орска. 2017 г.