УДК 343.988

О. А. Старостенко
старший преподаватель кафедры
оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

О ТИПОЛОГИИ ЖЕРТВ КИБЕРХИЩЕНИЙ В РОССИИ И ФАКТОРАХ, ПРОДУЦИРУЮЩИХ ИХ ВИКТИМНОСТЬ

Последовательное развитие отечественной криминологической мысли закрепило личность в качестве самостоятельного элемента предметной области практически всех дисциплин юридического цикла, образовав категорию личности преступника [1, с. 22]. Вместе с тем справедливо отмечает Л. В. Франк: «…действительно, если речь идет о значении личности преступника, то почему игнорируется личность жертвы? Ведь общественная опасность исходит не только от преступника, но и от жертвы» [2, с. 3]. Исходя из этого, формирование комплексной системы научного знания в области предупреждения преступлений и разработка мер антикриминальной практики не достижимы без информации о личности жертвы преступления.

Таким образом, изучение личности жертвы преступлений имеет важнейшее значение для юридической отрасли знания и практики предупреждения преступлений. Познание свойств личности жертвы дает возможность определить категорию граждан (выделить типологии), могущих становиться жертвами преступления, установить их гендерные, возрастные, профессиональные характеристики, а также выявить социальные и индивидуальные особенности виктимного поведения, которые следует учитывать при организации и осуществлении виктимологической профилактики преступлений.

В контексте дистанционных хищений личность жертвы выступает одним из ведущих элементов механизма совершения преступления. Проявляя неосмотрительность, она способствует запуску преступного поведения, нередко провоцирует злоумышленника на совершение противоправных действий, облегчает реализацию последовательных алгоритмов дистанционных хищений [3, с. 453]. В связи с этим виктимологическое предупреждение рассматриваемых преступлений невозможно без знаний типологии жертв и особенностей их виктимизации [4, с. 26].

Последовательное применение совокупности исследовательских операций (анализ 245 материалов уголовных дел, возбужденных на территории Российской Федерации; опрос 180 жертв дистанционных хищений;

140 сотрудников предварительного расследования; контент-анализ ресурсов сети Интернет; обобщение официальной статистической информации ГИАЦ Министерства внутренних дел России за 2018–2024 гг.) позволило определить, что всех жертв киберхищений можно условно разделить на две большие группы:

1. Жертвы хищений, совершенных путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях [5, с. 17], включая сеть Интернет (квалифицируются по ст. 158, 159; 159.3 Уголовного кодекса Российской Федерации). Данные преступления характеризуются предоставлением фиктивной информации, ее искажением с целью незаконного обогащения (механизм воздействия «человек — человек»).

2. Жертвы хищений, совершенных в сфере компьютерной информации (необходимо квалифицировать по ст. 159.6 Уголовного кодекса Российской Федерации). Преступление представляет собой несанкционированное вмешательство в работу программ и баз данных (механизм воздействия «человек — техника»).

Обобщение особенностей жертв дистанционных хищений, совершенных по схеме «человек — человек», позволяет определить отдельные их типы и установить особенности виктимизации.

1. Доверчивый тип жертвы характеризуется высокой степенью ее готовности верить в любые сведения, распространяемые в информационно-телекоммуникационной сети Интернет. Жертва отрицает возможность обмана и действует в соответствии с преступным сценарием. Жертва преступлений данного типа не видит причин для проверки подлинности URL-адресов, платежных форм и страниц сайтов, искренне веря в их подлинность. Безоговорочное исполнение алгоритма действий, включающих переход на фишинговый сайт и заполнение конфиденциальных данных в платежную форму, открывает объективную возможность для изъятия у жертвы денежных средств.

2. Корыстный тип жертвы представляет собой пользователя информационно-телекоммуникационной сети Интернет, склонного к постоянному извлечению материальной выгоды. Такие жертвы при получении «выгодного» материального предложения (акции, скидки), забывая о необходимости соблюдения правил информационной безопасности [6, с. 30], переходят на сомнительные ресурсы информационно-телекоммуникационной сети и передают конфиденциальные данные злоумышленникам.

3. Невнимательный тип жертвы характеризуется недостаточной сосредоточенностью в области обеспечения информационной и имущественной безопасности [7, с. 12]. Наряду с имеющимися у жертвы знаниями по обеспечению собственной защищенности в киберпространстве жертва данного типа

в связи с различными объективными обстоятельствами может не обратить внимание на подлинность URL-адреса, приняв его за оригинальный интернет-ресурс (например: www.mvidio.ru вместо www.mvideo.ru; www.aliiexpress.ru вместо www.aliexpress.ru и т. д.). Данный метод основывается на перехвате домена и называется киберсквоттинг.

Подводя итог рассмотрению особенностей жертв преступной схемы «человек — человек», отметим, что действия преступника часто зависят не только от его личностных особенностей, наклонностей и стремлений, но и от поведения жертвы. Жертва своими неосторожными, антиобщественными и аморальными поступками может создать провоцирующую, благоприятную для преступника обстановку, облегчающую наступление преступного результата.

Виктимологические особенности дистанционного хищения «преступник — техника» характеризуются отсутствием прямого взаимодействия преступника с жертвой. В таком случае для совершения хищения преступник воздействует на информационные ресурсы, средства и системы обработки информации либо использует иные технические устройства, которые позволяют создать благоприятные условия для преступления [8, с. 18]. Например, в информационную систему устанавливается вредоносное программное обеспечение, раскрываются учетные данные онлайн-банкинга, предоставляется доступ к удаленному управлению устройством, копируется либо фиксируется конфиденциальная информация, которая позволяет преступнику совершать дистанционное хищение.

Обобщение особенностей жертв дистанционных хищений, совершенных по схеме «человек — техника», позволяет определить их отдельную типологию.

1. Поведение жертвы характеризуется низким уровнем виктимности в силу должного уровня обеспечения личной имущественной и информационной безопасности. В целях обеспечения собственной информационной безопасности жертва использует различные лицензионные программы (например, антивирусы). Вместе с тем преступник, обладающий определенными познаниями в области IT, может преодолеть стандартные системы безопасности.

2. Жертва имеет средний уровень цифровой культуры, обладает общими знаниями в области информационной безопасности. В рамках данной типологии жертва зачастую пренебрегает правилами безопасности, что может спровоцировать или создать условия для совершения преступления.

3. Поведение жертвы характеризуется повышенным уровнем виктимности в силу отсутствия знаний в области обеспечения информационной

безопасности. Жертва создает условия для последующего преступного воздействия, провоцирует дистанционное хищение отсутствием защищенности используемого технического устройства.

Анализ преступной схемы «человек — техника» позволил установить, что при хищениях в сфере компьютерной информации зачастую наблюдается «размывание» субъекта индивидуальной виктимизации (физического лица, непосредственной жертвы преступления) [9].

В заключение хотелось бы остановиться на факторах объективного и субъективного характера, продуцирующих виктимность по отношению к преступлениям в киберпространстве.

В частности, к объективным факторам можно отнести:

1. Недостаточную защищенность инфраструктуры (уязвимости программного обеспечения и операционных систем).

2. Развитие технологий и расширение возможностей киберпреступников (появление новых видов вредоносного программного обеспечения, совершенствование методов социальной инженерии и др.).

3. Сложность раскрытия и расследования киберхищений (недостаток квалифицированных специалистов в правоохранительных органах, трудности в установлении личности и местонахождения преступников и др.).

4. Социально-экономические факторы (экономическая нестабильность, геополитическая напряженность).

К субъективным факторам можно отнести:

1. Недостаточную осведомленность и компетентность пользователей в вопросах кибербезопасности (например, отсутствие знаний об основных угрозах и методах защиты от них).

2. Доверчивость и невнимательность (разглашение личной информации в социальных сетях и на других онлайн-платформах).

3. Небрежность и халатность (использование незащищенных вайфай-сетей).

4. Зависимость от Интернета и социальных сетей (повышенная пользовательская сетевая активность).

Список основных источников

1. Аванесов Г. А. Криминология и социальная профилактика. М. : Акад. МВД СССР, 1980. 526 с. Вернуться к статье

2. Франк Л. В. Потерпевшие от преступления и проблемы советской виктимологии / Таджик. гос. ун-т им. В. И. Ленина. Душанбе : Ирфон, 1977. 237 с. Вернуться к статье

3. Репецкая А. Л., Петрякова Л. А. Виктимологическая характеристика мошенничеств в банковской сфере (по материалам Сибир. федер. округа) // Всерос. криминол. журн. 2022. Т. 16. № 4. С. 452–462. Вернуться к статье

4. Кабанов П. А. Жертвы киберкраж как объект современной российской кибервиктимологии: криминологический анализ статистических показателей криминальной виктимности 2021–2022 гг. // Виктимология. 2024. Т. 11. № 1. С. 25–42. Вернуться к статье

5. Кабанов П. А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021–2022 гг // Виктимология. 2023. Т. 10. № 1. С. 17–28. Вернуться к статье

6. Жмуров Д. В. Кибервиктимология как частная виктимологическая теория // Юрид. мир. 2024. № 7. С. 30–34. Вернуться к статье

7. Симоненко А. В., Соловьев В. С. Криминологический анализ показателей виктимизации российского общества // Общество и право. 2023. № 4(86). С. 8–14. Вернуться к статье

8. Вишневецкий К. В., Хомутов М. В. Факторы, влияющие на динамику виктимности // Юриспруденция: теория и практика. 2024. № 2. С. 16–22. Вернуться к статье

9. Старостенко О. А. Виктимологическое предупреждение дистанционных хищений / М. : Юрлитинформ, 2024. 152 с. Вернуться к статье