УДК 343.988(045)

О.А. Старостенко

ВИКТИМОЛОГИЧЕСКИЕ ОСОБЕННОСТИ СОВЕРШЕНИЯ ХИЩЕНИЙ ДИСТАНЦИОННЫМ СПОСОБОМ

В статье проведен анализ виктимологических особенностей механизма совершения дистанционных хищений. Выявлено, что алгоритмы совершения дистанционного хищения весьма многообразны – от элементарных примитивных до сложно выстроенных способов совершения преступления с использованием технологий больших данных, биометрии, таргетированной рекламы, искусственного интеллекта и программных ботов. На основании анализа и обобщения информации, полученной в ходе проведения опросов и изучения материалов уголовных дел (опрошено 182 сотрудника ОВД, изучено 80 уголовных дел) в области хищений, совершаемых дистанционно, определены модели виктимно-криминогенных ситуаций в зависимости от отдельных типов дистанционных хищений: «преступник – техника», «преступник – жертва – техника», «преступник – жертва». Тип «преступник – техника» характеризуется четырьмя основными моделями виктимно-криминогенных ситуаций. Виктимность жертвы в данном типе дистанционного хищения напрямую зависит от уровня цифровой культуры и киберграмотности личности. Тип «преступник – жертва – техника» характеризуется двумя моделями виктимно-криминогенных ситуаций. Виктимность жертвы в указанном алгоритме во многом зависит от уровня цифровой культуры и киберграмотности личности, от ее знаний в области обеспечения имущественной и информационной безопасности. Тип «преступник – жертва» характеризуется двумя моделями виктимно-криминогенных ситуаций соответственно. Виктимность жертвы преступления в контексте рассматриваемого вида дистанционного хищения не связана с киберграмотностью и цифровой культурой, а зависит от знаний в области личной имущественной безопасности, от степени доверчивости, алчности и заинтересованности жертвы в получении легкого дохода.

Ключевые слова: жертва, дистанционные хищения, интернет, информационно-телекоммуникационные технологии, виктимность, киберпространство.

DOI: 10.35634/2412-9593-2023-33-5-890-897

Традиционно механизм индивидуального преступного поведения рассматривается как взаимодействие внешних факторов объективной действительности и внутренних, психических процессов и состояний личности, определяющих преступное поведение [1, с. 112]. Разработанная В.Н. Кудрявцевым и дополненная А.И. Долговой концепция механизма преступного поведения включает ряд этапов криминального поведения, среди которых: формирование мотивации, принятие решения о совершении преступления, исполнение принятого решения, посткриминальное поведение [2, с. 58].

В контексте определения виктимологических особенностей механизма совершения дистанционных хищений приоритетное значение среди указанных этапов преступного поведения имеет процесс исполнения решения о совершении преступлений. В данном случае следует вести речь о конкретных способах совершения дистанционных хищений (далее – алгоритмах), знание которых позволит обеспечить качественную виктимологическую профилактику рассматриваемых преступлений, разработать направления ее реализации, передать населению знания в области обеспечения собственной безопасности от дистанционных хищений [3, 113–122].

Алгоритмы совершения дистанционного хищения весьма многообразны – от элементарных примитивных до сложно выстроенных способов совершения преступления с использованием технологий больших данных, биометрии, таргетированной рекламы, искусственного интеллекта и программных ботов. Алгоритм совершения дистанционного хищения может видоизменяться в зависимости от имеющихся у преступника знаний, умений и навыков в области использования IT-технологий, цели и объекта преступного посягательства, формирующейся криминогенной ситуации, социально-политической обстановки в государстве, виктимности личности и особенностей криминального взаимодействия преступника с жертвой. Криминальное взаимодействие преступника с жертвой нередко обусловлено виновной виктимностью жертвы, которая проявляет неосторожность, неосмотрительность, легкомысленность. Отсюда особый интерес представляют виктимологические особенности взаимодействия преступника с жертвой [4, с. 267–269].

Анализ и обобщение информации, полученной в ходе проведения опросов и изучения материалов уголовных дел (опрошено 182 сотрудника ОВД, изучено 80 уголовных дел) в области хищений,

совершаемых дистанционно, позволяют выявить виктимологические особенности механизма совершения дистанционных хищений. Они могут быть детально отражены в конкретных моделях виктимно-криминогенных ситуаций. Модели виктимно-криминогенных ситуаций представляют собой систему факторов, условий и обстоятельств, оказывающих решающее влияние на формирование у потенциальной жертвы качеств повышенной виктимности, а также реализацию преступного замысла злоумышленника [5, с. 31]. В контексте дистанционных хищений модели виктимно-криминогенных ситуаций можно выделить в зависимости от отдельных типов дистанционных хищений: «преступник – техника», «преступник – жертва – техника», «преступник – жертва».

1. Виктимологические особенности дистанционного хищения **«преступник – техника»** характеризуются отсутствием прямого взаимодействия преступника с жертвой. Для совершения хищения денежных средств преступник воздействует на информационные ресурсы, средства и системы обработки информации либо использует иные технические устройства, позволяющие в отсутствие взаимодействия с жертвой создать благоприятные условия для совершения преступления. В результате осуществления преступником указанных криминальных операций в информационную систему устанавливается вредоносное программное обеспечение, осуществляется неправомерный доступ к компьютерной информации, раскрываются учетные данные онлайн-банкинга, предоставляется доступ к удаленному управлению устройством, копируется либо фиксируется конфиденциальная информация, позволяющая преступнику совершать дистанционное хищение.

Виктимность жертвы в данном типе дистанционного хищения напрямую зависит от уровня цифровой культуры и киберграмотности личности.

Обобщение указанных виктимологических особенностей позволяет представить основные модели виктимно-криминогенных ситуаций дистанционного хищения, совершаемого по схеме «преступник – техника».

Модель 1. Жертва дистанционного хищения характеризуется низким уровнем виктимности в силу сформированной у нее цифровой культуры и киберграмотности, которые позволяют обеспечить ее безопасность в информационно-телекоммуникационном пространстве. В целях обеспечения собственной имущественной и информационной безопасности жертва использует совокупность различных лицензионных программных средств обеспечения IT-безопасности (например, антивирусы, шифрование, менеджеры паролей, антишпионы, родительский контроль и т. д.). Имеющиеся знания в области обеспечения информационной безопасности позволяют не допустить провокацию совершения хищения и препятствовать формированию криминогенной ситуации. Вместе с тем совершение дистанционного хищения все же возможно, и обусловлено это тем, что преступник, обладая специальными познаниями в области IT, преодолевает стандартные и высокозащищенные системы безопасности посредством высокоинтеллектуального (сложного) воздействия на средства обработки, хранения и передачи информации. Проведение длительной диагностики информационно-телекоммуникационного пространства и обнаружение уязвимостей позволяют преступнику осуществить неправомерное воздействие на информационные ресурсы, средства и системы обработки информации, в результате чего совершается незаконное изъятие денежных средств.

Модель 2. Жертва имеет средний уровень цифровой культуры и киберграмотности, обладает общими знаниями в области информационной безопасности. При ее обеспечении жертва нередко пренебрегает правилами защищенности информационных систем: использует нелицензированные продукты, чем нередко провоцирует и (или) создает условия для совершения хищения; ограничивается «стандартным набором» программных средств обеспечения IT-безопасности (антивирусы), не позволяющим в полной мере обеспечить имущественную и информационную защищенность; совершает единичные транзакции на неблагонадежных ресурсах сети Интернет, не имеющих технической возможности защитить конфиденциальные данные.

Подобное поведение позволяет преступнику преодолевать имеющуюся у жертвы систему обеспечения безопасности посредством высокоинтеллектуального (сложного) воздействия на средства обработки, хранения и передачи информации; использования уязвимостей в системе безопасности путем проведения типичных операций на основе поиска потенциальных жертв; внедрения в систему информационной безопасности жертвы вредоносных программных продуктов.

Модель 3. Поведение жертвы характеризуется высоким уровнем виктимности в силу отсутствия знаний в области обеспечения имущественной и информационной безопасности. Жертва самостоя-

тельно создает условия для последующего преступного воздействия, провоцирует дистанционное хищение отсутствием защищенности средств обработки и хранения информации, инсталляцией «пиратского» программного обеспечения, внедрением в информационную систему компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты. В контексте данной модели виктимно-криминогенной ситуации преступная деятельность реализуется посредством использования уязвимостей в системе безопасности, созданных непосредственно жертвой по причине игнорирования (либо незнания) основ обеспечения IT-защищенности путем предоставления относительно свободного доступа к объекту посягательства.

Модель 4. Уровень виктимности жертвы не зависит от цифровой культуры и киберграмотности личности. Жертва не провоцирует преступника и не создает условия для совершения в ее отношении дистанционного хищения. Преступная деятельность реализуется посредством использования различных технических устройств с целью перехвата конфиденциальной информации для последующего незаконного изъятия денежных средств. В качестве примера можно привести использование устройств считывания пин-кода на аппаратных средствах приема и выдачи денежных средств (банкоматах), установку видеонаблюдения с целью перехвата конфиденциальных данных, использование иных технических устройств для получения конфиденциальной информации и (или) непосредственного совершения хищения.

Выявленные модели виктимно-криминогенных ситуаций образуются при взаимодействии преступника с информационной системой, средствами хранения и обработки информации, воздействие на которые позволяет ему совершать хищение денежных средств посредством уникальных механизмов совершения преступления. Анализ судебно-следственной практики позволил определить наиболее характерные алгоритмы совершения дистанционного хищения в контексте указанных виктимно-криминогенных моделей.

Одним из наиболее распространенных алгоритмов совершения дистанционного хищения, посягающего на информационную систему, средства хранения и обработки информации, является совершение преступления посредством внедрения вредоносной компьютерной информации (программное обеспечение, файлы, иная компьютерная информация) в информационную систему или информационную инфраструктуру учреждений и организаций. Проникая в информационную систему, вредоносная компьютерная информация воздействует на функционирование средств хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей, открывает удаленный доступ к информационным системам, направляет злоумышленнику конфиденциальную информацию, относящуюся к банковским системам, платежным сервисам, пластиковым картам, позволяющую похитить денежные средства.

Согласно результатам анализа уголовных дел в исследуемой области, представленный алгоритм совершения дистанционного хищения был зафиксирован более чем в 40 % изучаемых материалов. Большинство таких преступлений посягает на юридических лиц (2/3). В данном случае вопросы виктимности юридических лиц и обеспечения их защищенности от дистанционных хищений требуют освещения в рамках отдельного виктимологического исследования.

Схожим алгоритмом совершения дистанционного хищения «преступник – техника» является осуществление неправомерного доступа к компьютерной информации с последующим совершением дистанционного хищения (без использования вирусного программного обеспечения). Объектами воздействия в данном случае выступают информационная инфраструктура кредитных организаций, оказывающих расчетные операции, маркетплейсов и классифайдов (сервисы объявлений), а также информационные системы иных компаний, собирающих и обрабатывающих конфиденциальные данные пользователей (например, данные пластиковых карт, логин и пароль от онлайн-банкинга, личного кабинета пользователя и т. д.). Преступник осуществляет неправомерный доступ к компьютерной информации путем подбора паролей, скрытого подключения к персональному компьютеру, использования уязвимостей в системе хранения и обработки информации, непосредственной эксплуатации персонального компьютера с конфиденциальной информацией. Осуществив неправомерный доступ к компьютерной информации и проникнув в информационную инфраструктуру указанных выше организаций, преступник получает конфиденциальные данные пользователей и распоряжается денежными средствами жертвы.

Наряду с представленными алгоритмами совершения дистанционного хищения «преступник – техника», не менее популярным является алгоритм, связанный с использованием иных технических устройств, позволяющих получать конфиденциальную информацию (скимминг). Преимущественным техническим устройством в контексте настоящего алгоритма совершения дистанционного хищения является скиммер. Это устройство, позволяющее считывать конфиденциальную информацию пластиковой карты [6]. Преступник использует различные виды скимминговых устройств (считыватель магнитной ленты, скрытая видеокамера, накладная клавиатура и т. д.), устанавливая их непосредственно на аппарат для выдачи и приема денежных средств. Жертва использует пластиковую карту, данные пластиковой карты считываются скимминговым устройством и сохраняются на носитель либо передаются злоумышленнику посредством радиоканалов, сотовой связи, беспроводных сетей. Заполучив указанную конфиденциальную информацию, преступник изготавливает дубликат пластиковой карты либо использует ее для непосредственного хищения денежных средств [7, с. 173–176].

2. Виктимологические особенности дистанционного хищения **«преступник – жертва – техника»** характеризуются непосредственным воздействием преступника на жертву и на средства обработки, хранения и передачи информации в результате использования высокоинтеллектуальных методов социальной инженерии, используемых при реализации преступных технологических решений. Виктимность жертвы во многом зависит от уровня цифровой культуры и киберграмотности личности, от ее знаний в области обеспечения имущественной и информационной безопасности. Знания в данной области позволяют жертве своевременно определять маркеры дистанционного хищения, избежать совершения преступного посягательства, иметь представление о порядке обращения в правоохранительные органы для защиты нарушенных прав. Нередко отсутствие знаний в области обеспечения личной имущественной и информационной безопасности способствует реализации преступного умысла злоумышленника. Реализация преступного механизма в контексте рассматриваемого вида дистанционных хищений обеспечивается как по схеме «преступник – жертва – техника», так и по схеме «преступник – техника – жертва». Изучение уголовных дел и проведенный в процессе исследования экспертный опрос демонстрируют, что хищения рассматриваемой категории составляют около 24 % от общего числа преступлений в исследуемой области.

Обобщение указанных виктимологических особенностей позволяет выделить две основные модели виктимно-криминогенных ситуаций дистанционного хищения, совершаемого по схеме «преступник – жертва – техника».

Модель 1. Жертва характеризуется средним уровнем виктимности в силу знания общих правил обеспечения личной имущественной и информационной безопасности, основ киберграмотности. Она не провоцирует совершение хищения и характеризуется нейтральным поведением. Преступная деятельность реализуется посредством введения жертвы в заблуждение с использованием высокоинтеллектуальных (сложных) программных средств и технологических решений совместно с методами социальной инженерии: разработка сайта, трудно отличимого от известных прототипов (например, www.leruamerlin.me вместо www.leroymerlin.ru; www.gosuslugis.com вместо www.gosuslugi.ru); создание иного интернет-ресурса, вводящего жертву в заблуждение (например, платежные формы «АvitoДоставка»); неправомерный доступ к социальным страницам пользователя с последующим хищением денежных средств у его знакомых.

Обобщение материалов судебной практики в области совершения дистанционных хищений позволяет определить, что указанная выше модель составляет 3 % от числа анализируемых преступлений.

Модель 2. Поведение жертвы характеризуется высоким уровнем виктимности в силу незнания общих правил обеспечения личной имущественной и информационной безопасности или их игнорирования. Наряду с тем, что жертва напрямую не провоцирует преступника, ее неосведомленность в области обеспечения IT-безопасности не позволяет своевременно выявить маркеры дистанционного мошенничества, в результате чего в отношении ее совершается преступление. Преступная деятельность реализуется посредством введения жертвы в заблуждение с использованием относительно простых программных средств и технических решений и строится на основе случайного (например, рассылка фишинговых писем посредством электронной почты, социальных сетей и мессенджеров) или персонализированного выбора жертвы.

Обобщение материалов судебной практики в области совершения дистанционных хищений позволяет определить, что указанная выше модель составляет 16 % от числа анализируемых преступлений.

Выявленные модели виктимно-криминогенных ситуаций образуются при взаимодействии преступника с жертвой посредством различных технологических решений и встроенных в них методов социальной инженерии. Подобные модели виктимно-криминогенных ситуаций содержат в себе ряд «классических» алгоритмов, которые могут видоизменяться в зависимости от познаний преступника в области IT, а также адаптироваться под общественно значимые события.

Анализ судебно-следственной практики позволяет определить наиболее характерные алгоритмы совершения дистанционного хищения в контексте указанных виктимно-криминогенных моделей и представить схемы их реализации.

Одним из наиболее популярных таких алгоритмов является совершение преступления посредством использования фишинговых ресурсов. По данным Центрального Банка России, в 2021 г. злоумышленники чаще всего маскировали фишинговые сайты под сайты действующих кредитно-финансовых организаций для получения персональных сведений пользователей или данных для входа в онлайн-банк, а также информации по банковским картам. Кроме того, злоумышленники активно использовали сайты с информацией о возможности получения компенсационных выплат от государства или о возможности заработать денежные средства за прохождение опроса, теста и т. п. Актуальным направлением в 2021 г. стали поддельные сайты известных маркетплейсов, магазинов по продаже электроники, бытовой техники, компьютеров и т. д. [8].

В период подготовки к совершению дистанционного хищения преступник избирает актуальное направление, продиктованное потребностями общества, политической обстановкой и (или) иными происходящими событиями (например, заработок в Интернете, оказание государственных услуг, прохождение вакцинации, отсрочка от мобилизации), на основе которого разрабатывает либо приобретает у третьих лиц образ официального интернет-ресурса, создавая поддельный (фишинговый) сайт либо платежную форму. Далее преступник наполняет фиктивный сайт контентом, оказывающим психологическое воздействие на жертву, с целью восприятия ей этого сайта в качестве официального интернет-ресурса, разрабатывает форму заполнения конфиденциальных сведений о банковских счетах, картах и (или) данных учетных записей онлайн-банкинга, организует рекламную компанию посредством имеющихся методов digital-маркетинга. Впоследствии жертва, заполняя указанную форму, передает информацию преступнику, в результате чего последний совершает хищение денежных средств [9, с. 17–28].

Наряду с вышеуказанной схемой совершения дистанционного хищения, распространенным алгоритмом совершения преступления является неправомерный доступ к компьютерной информации – социальным страницам лиц из числа «круга общения» жертвы с последующим хищением денежных средств под различными предлогами. Для этого преступник оказывает неправомерное воздействие на компьютерную информацию посредством высокоинтеллектуальных методов и технологических решений, получая доступ к социальным страницам отдельных лиц. Далее злоумышленник проводит анализ и оценку «круга знакомых», определяет потенциальную жертву преступления, осуществляет аналитическую деятельность, включающую изучение степени доверительности отношений между лицами, определение увлечений и интересов потенциальной жертвы, установление периодичности ее нахождения в онлайне. Осуществив сбор и обобщение информации о потенциальной жертве дистанционного хищения, преступник определяет наиболее эффективную стратегию взаимодействия с ней. Злоумышленник, вступая в коммуникацию с жертвой, как правило, осуществляет отправку сообщений с просьбой одолжить денежные средства, оказать финансовую помощь родственникам, друзьям и общим знакомым, пострадавшим в результате «квазипроисшествий». Находясь под воздействием обмана, жертва совершает перевод денежных средств на банковский счет или карту преступника.

Одним из новаторских алгоритмов дистанционного хищения «преступник – жертва – техника», представленных специалистами в ходе экспертного опроса, является совершение преступления посредством инсталляции жертвой программного обеспечения удаленного доступа к устройству. Криминальное воздействие направлено в первую очередь на личность, и лишь затем на средства обработки, хранения и передачи информации. Сначала преступник устанавливает межличностную коммуникацию посредством мобильной связи, представляясь сотрудником банковской организации. Далее, используя методы социальной инженерии, он уведомляет и внушает жертве необходимость обновления программного обеспечения банковского обслуживания (например, «ВТБ Онлайн», «Сбербанк Онлайн» и т. д.) посредством скачивания «банковского» квазиприложения (например, «ВТБподдержка»). В результате выполнения последовательных действий по установке указанного ПО, жертва инсталлирует

в мобильное устройство приложение удаленного доступа. Завершив процесс установки, жертва сообщает идентификационную информацию «сотруднику банка», в результате чего преступник получает возможность удаленного управления устройством, изымает конфиденциальную информацию (например, логины и пароли, данные банковских карт, учетные сведения в онлайн-банкинге и т. д.) и завладевает денежными средствами.

3. Виктимологические особенности хищений по схеме **«преступник – жертва»** выражаются в непосредственном психологическом воздействии на жертву средствами социальной инженерии, позволяющими вводить ее в заблуждение. Такое воздействие обеспечивается использованием информационно-телекоммуникационных технологий и средств мобильной связи при отсутствии незаконного вмешательства в процессы их функционирования. Виктимность жертвы преступления в контексте рассматриваемого вида дистанционного хищения не связана с киберграмотностью и цифровой культурой, а зависит от знаний в области личной имущественной безопасности, от степени доверчивости, алчности и заинтересованности жертвы в получении легкого дохода. Изучение уголовных дел и проведенный в процессе исследования экспертный опрос демонстрирует, что указанные преступления составляют 68 % от общего количества дистанционных хищений. Это обусловлено доступностью, простотой осуществления преступления, низкой степенью технологического оснащения и минимальными рисками изобличения преступника.

Обобщение указанных виктимологических особенностей позволяет выделить две основные модели виктимно-криминогенных ситуаций дистанционного хищения, совершаемого по схеме «преступник – жертва».

Модель 1. Поведение жертвы характеризуется средним уровнем виктимности в силу знания общих правил обеспечения личной имущественной и информационной безопасности. Преступная деятельность реализуется посредством введения жертвы в заблуждение с использованием сложных (многоступенчатых) технологий социальной инженерии. Здесь следует вести речь о том, что преступное посягательство совершается поэтапно и в первую очередь направлено на получение информации о жертве, а именно: наличии открытых счетов в банках, имеющихся дебетовых и кредитных картах, пользовании услугами интернет-банкинга, существующих проблемах в обслуживании и т. д. Далее преступник обращается к программным средствам, позволяющим получать информацию о владельце номера телефона из открытых источников (например, «Getcontact», «ГлазБога»), которые позволяют узнать регион, в котором зарегистрирована симкарта, ФИО владельца номера, наименование его номера в телефонной книге третьих лиц, адрес страницы в социальных сетях и фотоизображения. Нередко сбор информации преступником сопровождается анализом социальной страницы жертвы с целью определения ее потребностей, интересов и увлечений. В совокупности анализ получаемой преступником информации позволяет ему определить наиболее «удачную» тактику осуществления дистанционного хищения, подобрать конкретные методы социальной инженерии и «успешно» совершить преступление. В контексте рассматриваемой модели наиболее популярной уловкой преступника является криминальное давление на человеческие слабости (любопытство, страх, беспечность, корысть и т. д.).

Обобщение материалов судебной практики в области совершения дистанционных хищений позволяет определить, что указанная выше модель составляет 6 % от числа анализируемых преступлений.

Модель 2. Поведение жертвы характеризуется высоким уровнем виктимности в силу незнания общих правил обеспечения личной имущественной и информационной безопасности, излишней доверчивости, заинтересованности в получении «легкого» заработка. Преступная деятельность реализуется посредством создания квазиобъявлений на соответствующих сервисах сети Интернет, недобросовестных магазинов на платформах электронной коммерции (маркетплейсы) либо в результате отклика преступника на размещаемые жертвой объявления, телефонных звонков и других средств коммуникации, позволяющих вводить жертву в заблуждение путем использования простейших форм обмана и технологий социальной инженерии.

Обобщение материалов судебной практики в области совершения дистанционных хищений позволяет определить, что указанная выше модель составляет 66 % от числа анализируемых преступлений.

Выявленные модели виктимно-криминогенных ситуаций образуются при взаимодействии преступника с жертвой посредством «классических» средств коммуникации (как, например, средства сотовой и мобильной связи) и традиционных интернет-ресурсов (мессенджеры, социальные сети и т. д.). Указанные модели содержат несколько типичных алгоритмов совершения дистанционного хищения.

Наиболее популярным алгоритмом совершения преступления является дистанционное хищение, совершаемое посредством мобильной связи. Здесь следует вести речь о двух основных типах преступных алгоритмов.

Первый алгоритм характеризуется серьезной подготовкой преступника к совершению преступления и включает в себя: получение информации о потенциальной жертве, ее местонахождении, близких родственниках, увлечениях, наличии карт, счетов и кредитных продуктов в банках и т. д. Основными источниками получения указанной выше информации являются бесконтрольно распространенные либо украденные данные клиентов, социальные сети, telegram-боты и иные инструменты, позволяющие получить информацию о жертве из открытых источников. Отталкиваясь от полученной информации, преступник избирает наиболее «удачную» стратегию взаимодействия, эффективные методы социальной инженерии и вступает в коммуникацию посредством мобильной связи с жертвой с целью хищения у нее денежных средств.

Второй алгоритм представляет собой аналогичную схему совершения дистанционного мошенничества посредством мобильной связи. Его отличительной особенностью является лишь то, что преступник не готовится к совершению преступления, порядок преступных действий хаотичен и определяется в процессе коммуникации с жертвой преступления в зависимости от складывающейся обстановки.

Указанный криминальный алгоритм является одним из наиболее распространенных не только в рамках дистанционного хищения «преступник – жертва» (около 40 % от исследуемых материалов судебной практики), но и среди остальных видов рассматриваемого преступления.

Наряду с дистанционным хищением «преступник – жертва», совершаемым посредством мобильной связи, распространенным алгоритмом является хищение денежных средств в результате отклика преступника на объявление о продаже товаров, размещенное жертвой на классифайдах. Преступная деятельность в данном алгоритме реализуется последовательным анализом преступником интернет-ресурсов по размещению объявлений о продаже товаров и (или) оказании услуг. Злоумышленник определяет жертву и вступает с ней в коммуникацию посредством мобильной связи. В результате общения преступник, используя методы и приемы социальной инженерии и воздействуя на психологическое состояние жертвы, уговаривает ее передать конфиденциальные данные платежных карт либо перевести денежные средства под различными предлогами.

Менее распространенным является алгоритм совершения преступления посредством создания объявлений на классифайдах и маркетплейсах. В данном случае преступник, используя какую-либо из сервисных платформ для размещения объявлений и (или) продажи товаров, разрабатывает объявление и составляет описание товаров и (или) услуг. Откликаясь на указанное объявление, жертва вступает в коммуникацию с преступником, проводит оплату (предоплату) за товар либо услуги. После получения денежных средств преступник прекращает общение, тем самым совершает незаконное хищение денежных средств.

Представленные характеристики жертв дистанционных хищений позволяют определить основные типы указанных преступлений, основываясь на которые следует формировать механизм предупредительной деятельности, направленный на минимизацию криминогенных факторов [10, с. 26].

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Кудрявцев В.Н. Механизм преступного поведения // Юридическая психология / под ред. Т.Н. Курбатовой. СПб.: Питер, 2001. 248 с.
2. Криминология: учеб. для вузов / под общ. ред. А.И. Долговой. 3-е изд., перераб. и доп. М.: Норма, 2005. 912 с.
3. Жмуров Д.В. Кибервиктимность как новая категория виктимологии постмодерна // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. 23 (2). С. 113–122.
4. Старостенко О.А. Виктимологическая характеристика мошенничества, совершаемого с использованием информационно- телекоммуникационных технологий // Гуманитарные, социально-экономические и общественные науки. 2020. № 5. С. 267–269.
5. Майоров А.В. Модель развития виктимологической ситуации // Виктимология. 2018. № 1. С. 30–36.
6. Считать и украсть: как работает скимминг банковских карт. URL: https://trends.rbc.ru/trends/industry/612d019d9a79470c54677745.
7. Жмуров Д.В. Исследование потерпевших в интернете как один из элементов превенции киберпреступности // Научное обеспечение раскрытия, расследования и предупреждения преступлений : Материалы Всероссийской научно-практической конференции к юбилею доктора юридических наук, профессора, заслуженного

юриста Российской Федерации Александра Алексеевича Протасевича, Иркутск, 15 декабря 2022 года. Иркутск: Байкальский государственный университет, 2023. С. 173–176.
8. Банк России. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году. URL: https://www.cbr.ru/analytics/ ib/operations_survey_2021/.
9. 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.
10. Грибанов Е.В. Универсальная (типовая) технология предупреждения преступлений // Общество и право. 2021. № 3 (77). С. 26–31.

Поступила в редакцию 25.08.2023

Старостенко Олег Александрович, преподаватель кафедры оперативно-разыскной деятельности
ФГКОУ ВО «Краснодарский университет Министерства внутренних дел Российской Федерации»
350005, Россия, г. Краснодар, ул. Ярославская, 28
E-mail: olegstaros94@gmail.com

O.A. Starostenko

VICTIMOLOGICAL FEATURES OF COMMITTING THEFT BY REMOTE MEANS

DOI: 10.35634/2412-9593-2023-33-5-890-897

The article analyzes the victimological features of the mechanism of remote theft. It has been revealed that the algorithms for committing remote theft are very diverse – from elementary primitive to complex ways of committing a crime using big data technologies, biometrics, targeted advertising, artificial intelligence and software bots. Based on the analysis and generalization of information obtained during surveys and the study of criminal case materials (182 police officers were interviewed, 80 criminal cases were studied) in the field of theft committed remotely, models of victim-criminogenic situations were determined depending on certain types of remote theft: "criminal – technique", "criminal – victim – technique", "criminal – victim". The "criminal – technique" type is characterized by four main models of victim-criminogenic situations. Victimization of the victim in this type of remote theft directly depends on the level of digital culture and cyber literacy of the individual. The "criminal – victim – technique" type is characterized by two models of victim-criminogenic situations. Victimization of the victim in this algorithm largely depends on the level of digital culture and cyber literacy of the individual, on his/her knowledge in the field of property and information security. The "criminal – victim" type is characterized by two models of victim-criminogenic situations, respectively. Victimization of the victim of a crime in the context of the considered type of remote theft is not related to cybercrime and digital culture, but depends on knowledge in the field of personal property security, on the degree of credulity, greed and interest of the victim in obtaining an easy income.

Keywords: victim, remote theft, Internet, information and telecommunication technologies, victimization, cyberspace.

Received 25.08.2023

Starostenko O.A., Lecturer of the Department of Operational Investigative Activities
Krasnodar University of the Ministry of Internal Affairs of the Russian Federation
Yaroslavskaya st., 128, Krasnodar, Russia, 350005
E-mail: olegstaros94@gmail.com