живаются и фиксируются также признаки бризантного и термического воздействия взрыва, следы разлета фрагментов ВУ, собираются части непрореагировавшего ВВ, фрагменты промышленной упаковки ВВ, обрывки бумаги и картона, мелкие фрагменты ВУ.

Во второй и третьей пространственных зонах на предметах обстановки обнаруживаются и фиксируются признаки фугасного и сейсмического воздействия взрыва, следы разлета фрагментов ВУ, берутся контрольные пробы грунта, штукатурки, а также образцы от предметов, имеющих общую родовую принадлежность с предметами-носителями микрочастиц и микрокоследов ВВ и неподвергавшихся действию взрыва (аналогичные обои, паркет, доски и другие предметы и материалы без следов взрыва).

Остатки и микрообъекты непрореагировавшего ВВ, конденсированные продукты взрыва, фрагменты оболочки ВУ, объекты-носители микрочастиц и микрокоследов ВВ изымаются в резиновых перчатках с применением пинцетов, игл, ножей, лопаток, тампонов и т. п. Обнаруженные объекты упаковываются раздельно, в герметичные стеклянные, полиэтиленовые бюксы и коробки, либо при их отсутствии в герметичные полиэтиленовые пакеты. Бумажная упаковка крайне нежелательна, поскольку ВВ и продукты взрыва способны быстро улетучиваться.

Таким образом, только тактически грамотные и организационно выверенные действия участников осмотра будут способствовать извлечению максимального объема криминалистически значимой информации из среды события преступления, характеризующейся расширенными пространственными аспектами и особыми правилами и условиями работы.

УДК 343.7

М.М. Савченко

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА СПОСОБОВ СОВЕРШЕНИЯ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ

Современные тенденции увеличения количества денежных расчетов с использованием дистанционных банковских технологий одновременно обусловливают стремительный рост преступных посягательств на денежные средства граждан, размещенных на счетах и банковских платежных карточках. Рост количества таких преступлений ускорился в первые месяцы пандемии COVID-19 [1].

Для разработки мероприятий для предотвращения данных деяний, а также для разработки методик расследования преступлений необходимо провести систематизацию способов их совершения.

Проведем классификацию способов совершения преступлений указанной группы в зависимости от технологии обработки платежной информации [2]:

1. Неправомерное осуществление наличных расходных операций в кассе банка неуполномоченными лицами от имени клиента.

2. Постоянное или временное физическое завладение чужой банковской платежной карточкой и ее неправомерное использование для осуществления операций.

3. Копирование информации с банковской платежной карточки, ее электронной полосы, а также ее реквизитов, достаточных для осуществления расходных операций.

4. Неправомерное завладение кодами (из СМС-сообщений, таблиц разовых ключей и т. д.), являющимися аналогами электронной цифровой подписи, позволяющими совершить одну или несколько конкретных банковских операций.

5. Неправомерное завладение информацией, позволяющей использовать все возможности дистанционного банковского обслуживания от имени клиента.

6. Введение клиента банка в заблуждение с последующим побуждением к совершению безналичных расходных операций в пользу виновных лиц и их сообщников.

Следует отметить, что вышеуказанная классификация проведена в зависимости от путей завладения виновными лицами платежной информации, однако в рамках некоторых видов возможна уголовно-правовая квалификация деяний по различным статьям Уголовного кодекса Российской Федерации (УК РФ) [3]. Основными нормами, предусматривающими ответственность за такие деяния, являются:

п. «г» ч. 3 ст. 158 «Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3)» УК РФ;

ст. 159.3 «Мошенничество с использованием электронных средств платежа» УК РФ;

ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ.

Разграничение данных составов между собой в некоторых случаях является сложной задачей [4–6]. В целях обеспечения единообразия судебной практики по рассматриваемой категории дел Верховным Судом

(ВС) РФ было принято соответствующее постановление от 30 ноября 2017 г. № 48 [7], однако постоянное совершенствование информационных технологий банковского обслуживания обусловливает появление новых способов совершения хищений в данной сфере, что ставит все новые вопросы в правоприменительной практике.

Пункт «г» ч. 3 ст. 158 УК РФ является квалифицированным составом преступления, предусмотренного ч. 1 ст. 158 «Кража – тайное хищение чужого имущества» УК РФ. Анализ диспозиции данной статьи позволяет сделать вывод, что под ее действия попадают исключительно случаи тайного хищения, что подтверждается практикой ВС РФ (п. 2 постановления Пленума ВС РФ от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» [8]).

Как тайное хищение чужого имущества (кража) следует квалифицировать действия лица, совершившего незаконное изъятие имущества в отсутствие собственника или иного владельца этого имущества, или посторонних лиц либо хотя и в их присутствии, но незаметно для них.

Хищение, совершенное с физическим использованием банковских платежных карточек, может быть квалифицировано в зависимости от способа реализации преступного замысла либо по п. «г» ч. 3 ст. 158, либо по ст. 159.3 УК РФ.

Преступник может завладеть банковской платежной карточкой различными способами: украсть, найти чужую, временно тайно завладеть чужой; получить путем удержания ее в фиктивном банкомате или специальном устройстве, устанавливаемом на настоящий банкомат.

В случае если лицо, завладевшее банковской платежной карточкой, тайно осуществляет расходную операцию в банкомате, получая наличные денежные средства либо перечисляя их безналичным платежом на свой счет, данное деяние следует рассматривать как кражу по соответствующей части ст. 158 УК РФ. Состава мошенничества не образует также ситуация, при которой злоумышленник обманом выясняет пин-код банковской платежной карточки. Данная позиция подтверждается п. 2 постановления ВС РФ от 30 ноября 2017 г. № 48: «если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного в зависимости от способа хищения образуют состав кражи или грабежа».

Деяния, связанные с копированием банковских платежных карточек, получением информации о секретных кодах (CVV/CVC) или с магнитной полосы, подлежат юридической квалификации в зависимости от способа дальнейшего использования полученных данных. Квалификация осуществляется аналогично операциям с физической карточкой как

кража или мошенничество по ст. 159.3 либо ч. 3 ст. 159.6 УК РФ в зависимости от того, каким образом используется поддельная карточка – для получения наличных денег или оплаты товаров и услуг. «В случаях, когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя банковской карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карточки под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кража».

В последнее время количество совершенных таким способом деяний сокращается, так карточки без чипа (только с магнитной полосой) российскими банками почти не выдаются, а копирование карточек с чипом технически невозможно. При использовании реквизитов банковской платежной карточки, в том числе секретных кодов, при оплате товаров, банками почти повсеместно используется дополнительная технология защиты 3dSecurity, а при ее отсутствии у владельца счета имеется возможность отмены операции.

Квалификация деяний, связанных с завладениями информацией и (или) кодами, являющимися аналогом простой неквалифицированной электронно-цифровой подписи, зависит от установления следующих обстоятельств:

каким способом получена вышеуказанная информация/коды;

каким образом использована эта информация/коды.

Коды для подтверждения операции могут быть получены следующими способами:

при использовании вредоносных компьютерных программ;

при использовании потерпевшим поддельных ссылок на страницы с формами оплаты товаров или услуг;

при неправомерном завладении абонентским устройством потерпевшего, в том числе при незаконном перевыпуске сим-карты;

простым подсматриванием кодов;

при введении в заблуждение потерпевшего относительно назначения кода (например, потерпевший думает, что это код, необходимый для получения денег на счет, либо код для отмены операции).

Проведенная в данной работе классификация способов совершения хищений с банковских счетов физических лиц может стать основой для планирования первоначальных следственных действий и определения источников получения доказательств при расследовании уголовных дел.

1. Сухаренко, А.Н. Криминальные вызовы пандемии COVID-19 в России : науч.-практ. пособие / А.Н. Сухаренко, М.М. Савченко, Ю.В. Трунцевский. – М. : Проспект, 2021. – 336 с.

2. Савченко, М.М. Проблемы уголовно-правовой защиты безопасности денежных средств физических лиц, размещенных на счетах в банках / М.М. Савченко // Юрид. образование и наука. – 2021. – № 4. – С. 34–40.

3. Уголовный кодекс Российской Федерации // СПС «КонсультантПлюс».

4. Хисамова, З.И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики / З.И. Хисамова // Рос. следователь. – 2018. – № 9. – С. 43–47.

5. Яни, П. Мошенничество с использованием электронных средств платежа / П. Яни // Законность. – 2019. – № 5. – С. 25–28.

6. Савченко, М.М. Правовая природа безналичных и электронных денег как предмета преступных посягательств / М.М. Савченко // Бизнес. Образование. Право. – 2021. – № 2 (55). – С. 118–124.

7. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс] : постановление Пленума Верхов. Суда Рос. Федерации, 30 нояб. 2017 г., № 48 // СПС «КонсультантПлюс».

8. О судебной практике по делам о краже, грабеже и разбое [Электронный ресурс] : постановление Пленума Верхов. Суда Рос. Федерации, 27 дек. 2002 г., № 29 // СПС «КонсультантПлюс».

УДК 343.985

С.С. Сенькевич

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЦИФРОВОЙ КРИМИНАЛИСТИКИ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ О НЕЗАКОННОЙ ОХОТЕ

С ежедневным расширением использования в различных сферах жизнедеятельности человека цифровых технологий, к сожалению, следует констатировать факт процесса использования того же инструментария в противоправной деятельности преступных элементов. Не остается в стороне и преступная деятельность, связанная с осуществлением незаконной охоты. Особый импульс развития информационные технологии получили в период пандемии COVID-19.

К сожалению, традиционные методы криминалистики, связанные с поиском и обнаружением следов преступной деятельности, в цифровом пространстве оказываются не всегда эффективными. В связи с чем в настоящее время получило бурное развитие отдельное направление – цифровая криминалистика. По нашему мнению, к цифровым следам необходимо в первую очередь относить информацию, связанную с событием преступления, отраженную в материальной среде, которая возникла, обрабатывается, распространяется и хранится посредством использования в указанных процессах информационно-коммуникативных технологий. Специфика образования информации, ее распространение, хранение и модификация в первую очередь и предопределяют развитие новых форм поиска, обнаружения и фиксации, как имеющей доказательственное значение по уголовному делу, а также, в свою очередь, придают импульс в развитии соответствующей криминалистической техники.

Специфика работы с такими следами также связана с возможностью их модификации, удаления, со стороны преступников, соответственно, работа с ними сопряжена с привлечением специалиста, обладающего специальными знаниями в указанной области и соответствующего оборудования.

В настоящее время преступники, осуществляющие незаконную охоту, все чаще для достижения преступного результата используют радиосвязь, электронные, оптические и поисковые приборы, что, в свою очередь, не оставляет ни единого шанса животному. Современное состояние мобильных сетей обеспечивает покрытие Республики Беларусь почти по всей территории, общедоступность интернета и его достаточно быстрая скорость обеспечивают возможность связи между участниками незаконной охоты посредством социальных сетей, с использованием мессенджеров, с возможностью передачи не только текстовых, голосовых сообщений, но и видеофайлов, в режиме практически реального времени, что, в свою очередь, также предопределяет эффективность преступной деятельности.

Все большую популярность в настоящее время приобретают GPS-трекерры, использование которых в режиме реального времени позволяет на мобильном устройстве отследить местонахождение собаки, осуществляющей загон животного.

Особого внимания заслуживает использование квадрокоптера с целью отыскания зверя, а также с целью обеспечения «безопасности» осуществляемых противоправных действий, обнаружения представителей правоохранительных органов в районе совершения преступления, иных лиц, находящихся в непосредственной близости к месту совершения преступления.

Не является редкостью размещение преступниками в социальных сетях фотографий и видеоматериалов с незаконной охотой, либо законной охоты, но позволяющих по их метаданным определить, что в момент