

Отдельно следует остановиться на ряде научных направлений, которые еще не получили признания самостоятельных отраслей криминалистической техники, однако рассматриваются в качестве таковых некоторыми учеными.

В первую очередь речь идет о разработке теории криминалистического исследования электронно-цифровой техники, программных средств и компьютерной информации. Значительный вклад в развитие данного направления криминалистики внесли труды В.Б. Вехова, В.В. Крылова, Н.С. Полевого, Е.Р. Россинской, А.И. Усова и других ученых. Вместе с тем, по нашему мнению, пока преждевременно говорить о том, что научные основы этого направления сформировались, поскольку не выработано его единое наименование (в качестве таковых предлагается «криминалистическое исследование компьютерной информации и техники» [6], «криминалистическое исследование электронных носителей информации» [14], «судебная дигитология» [15]), не определены предмет, объект и решаемые задачи.

Таким образом, следует констатировать, что в настоящее время отрасли криминалистической техники, их теоретическое и практическое наполнение находятся в процессе переосмысления и дополнения. Этот процесс – объективная закономерность, обусловленная прямой зависимостью криминалистики от перманентного развития науки и техники в целом; закономерность, которую следует принять и учитывать, чтобы своевременно и оперативно реагировать на возникающие перед научным криминалистическим сообществом вызовы.

1. Проблемы использования цифровой фотографии в досудебном производстве / В.А. Газизов [и др.] // Судебная экспертиза: дидактика, теория, практика : сб. науч. тр. М., 2005. С. 131–134.

2. Ростовцев А.В. Технично-криминалистические методы контроля изменений цифровых изображений в судебной фотографии // Изв. Тул. гос. ун-та. Эконом. и юрид. науки. 2010. Вып. 1, ч. 1. С. 358–361.

3. Глушков М.Р. Совершенствование правового и методического обеспечения видеозаписи при производстве следственных действий : дис. ... канд. юрид. наук : 12.00.12. М., 2018.

4. Галяшина Е.И. Теоретические и прикладные основы судебной фоноскопической экспертизы : дис. ... д-ра юрид. наук : 12.00.09. Воронеж, 2002.

5. Криминалистика : учебник для вузов / Т.В. Аверьянова [и др.]. 4-е изд., перераб. и доп. М., 2020.

6. Криминалистика : учебник / Н.П. Яблоков [и др.]; под ред. Н.П. Яблокова. 4-е изд., перераб. и доп. М., 2019.

7. Аминев Ф.Г. О современных возможностях криминалистического исследования трасологических объектов // Эксперт-криминалист. 2011. № 3. С. 28–29.

8. Лузгин И.И. Криминалистика : учеб.-метод. комплекс для студентов спец. 1-24 01 «Правоведение» : в 5 ч. Новополюк, 2008–2009. Ч 2 : Криминалистическая техника и системная технология (Криминалистическое исследование материальной структуры преступления) : в 2 кн. Кн. 1. 2008.

9. Судебная баллистика и судебно-баллистическая экспертиза : учебник / А.Г. Егоров [и др.]. – Саратов, 1998.

10. Беляков А.А. Взрывчатые вещества и взрывные устройства (криминалистическая взрывотехника). М., 2003.

11. Поваркова Е.А. Актуальные проблемы криминалистической регистрации // Проблемы отправления правосудия по уголовным делам в современной России: теория и практика : сб. науч. ст. IV Междунар. науч.-практ. конф., Курск, 16–18 апр. 2015 г. : в 2 ч. Курск, 2015. Ч. 2. С. 163–167.

12. Мартынов Ю.Р. Криминалистическая регистрация: проблемы, тенденции, перспективы // Правовые, социально-гуманитарные и экономические проблемы в фокусе научных исследований : материалы Всерос. науч.-практ. конф., Хабаровск, 12 нояб. 2016 г. Хабаровск, 2016. С. 245–250.

13. Шведова Н.Н. Отдельные теоретические вопросы криминалистического исследования документов как раздела криминалистической техники // Актуал. проблемы рос. права. 2015. № 4. С. 125–130.

14. Демин К.Е. К вопросу о выделении криминалистического исследования электронных носителей информации как новой отрасли криминалистической техники // Библиотека криминалиста. 2013. № 5. С. 174–180.

15. Романенко М.А. Судебная дигитология – современный взгляд на содержание криминалистической техники // Вестн. Ом. ун-та. Серия «Право». 2007. № 1. С. 147–155.

УДК 343.4

А.В. Ивановский, С.А. Черняк

ПРОБЛЕМЫ ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ ХИЩЕНИЙ ПУТЕМ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ТЕХНИКИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Развитие информационных технологий создало и условия для совершения в киберпространстве преступлений (Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. ... канд. юрид. наук : 12.00.08. М., 2016.). Примером тому может служить развитие безналичных расчетов и интернет-торговли, которые в связи с низкой компьютерной и финансовой грамотностью населения республики несут значительные преступные риски в сфере высоких технологий. Поэтому на фоне стойкого снижения общего

уровня преступности в Республике Беларусь растет число преступлений в сфере высоких технологий, среди которых лидирует хищение путем использования компьютерной техники (ст. 212 Уголовного кодекса Республики Беларусь (УК)). Так, за 2017 г. в республике зарегистрировано 2 318 таких преступлений; в 2018 г. – 3 585; в 2019 г. – 8 047. За 8 месяцев 2020 г. зарегистрировано 7 417 преступлений данного вида, и, исходя из динамики их развития, можно прогнозировать их значительный рост и в дальнейшем.

С момента создания и функционирования в республике подразделений по раскрытию преступлений в сфере высоких технологий (с 2002 г. в МВД и с 2004 г. в УВД облисполкомов) можно отчетливо проследить эволюцию развития и изменения способов хищений с использованием компьютерной техники.

На начальном этапе – в 2000-е гг. – преобладали хищения с помощью подлинных банковских платежных карточек (БПК), неправомерно вышедших из законного владения их держателей, а также с помощью банкоматов. Позже добавились хищения с использованием реквизитов БПК, т. е. через получение информации, записанной на магнитной полосе скиммеров (миниатюрных переносных считывающих устройств, устанавливаемых на банкоматах), и нанесение ее на поддельные карточки. На протяжении последних 5 лет стали преобладать хищения посредством получения обманным путем (используется вишинг, фишинг, социальная инженерия) в социальных сетях, мессенджерах или на торговых площадках в сети Интернет таких реквизитов БПК, как номер карты, фамилия и имя держателя, срок действия и проверочный код.

Проведенный анализ всех хищений с использованием компьютерной техники за 8 месяцев 2020 г. в Гродненской области показал, что около 70 % таких преступлений совершаются через завладение обманным путем реквизитов БПК в социальных сетях и на торговых площадках и только 30 % – с использованием подлинных БПК и банкоматов. Таким образом, отчетливо прослеживается зависимость эволюции хищений от развития информационных ресурсов и платежных инструментов.

Рассматривая уголовно-правовые нормы, регулирующие правоотношения, связанные с хищением путем использования компьютерной техники (ст. 212 УК), необходимо констатировать, что они остались практически неизменными с момента принятия УК (изменения вносились только один раз – в 2016 г., когда был снижен возраст привлечения к уголовной ответственности с 16 до 14 лет).

В ходе практической деятельности по применению указанных норм права у правоохранителей возникает ряд проблемных (спорных) вопросов.

Диспозиция ст. 212 УК предусматривает уголовную ответственность за совершение двух фактически разных видов противоправных деяний, различающихся по своей сути, способу совершения и степени общественной опасности: хищения денежных средств с карт-счетов, связанного с использованием похищенных либо утраченных подлинных банковских платежных карточек, их реквизитов и банкоматов, и хищения денежных средств, сопряженного с копированием реквизитов банковских пластиковых карточек, изготовлением и использованием поддельных карточек.

Следует разделить данные два вида противоправных деяний, отразив их в различных статьях УК. Для хищений, сопряженных с использованием подлинных банковских платежных карточек и их реквизитов, возможно оставить ст. 212 УК, соответственно изменив ее диспозицию, для действий, связанных с кардингом (копированием реквизитов БПК, изготовлением и использованием поддельных карточек), – ввести новую статью в УК. При этом в новой статье следует предусмотреть уголовную ответственность за любые действия, направленные на хищения (завладение реквизитами БПК, изготовление и сбыт поддельных банковских карточек, использование поддельных карточек), а также разграничить ответственность в зависимости от суммы хищения и иных квалифицирующих признаков. Данная статья ввиду направленности противоправных деяний на завладение, копирование и использование компьютерной информации может быть отнесена к гл. 31 УК.

Еще одной давней проблемой правоприменительной практики является различный субъективный подход при возбуждении уголовных дел по ст. 212 УК, если сумма похищенного незначительна – до 1 базовой величины (БВ). Так, например, за 5 месяцев 2020 г. подразделениями Следственного комитета Гродненской области возбуждено 31 уголовное дело по ч. 2 ст. 212 УК, по которым ущерб составил менее 1 БВ (27 руб.). По 15 уголовным делам данной категории установлены подозреваемые лица. Необходимо отметить, что еще по 5 возбужденным уголовным делам приняты решения об отмене постановлений о возбуждении дела на основании п. 9 ст. 179 УПК и о прекращении на основании п. 2 ч. 1 ст. 29 УПК (суммы похищенного по указанным делам составили от 4,09 до 11,66 руб.).

При этом можно выявить следующую закономерность: с незначительными суммами похищенного уголовные дела безоговорочно возбуждаются в отношении неустановленного лица и с определенными трудностями – при наличии подозреваемого лица (как правило, такие материалы возвращаются в ОВД для проведения дополнительной проверки, либо подразделения СК принимают решения, не связанные с возбуждением уголовного дела, со ссылкой на малозначительность).

Для решения данной проблемы правоприменительной практики в случае хищений, совершенных с использованием подлинных БПК, если сумма похищенного незначительна, назрела необходимость применения ч. 4 примечаний к гл. 24 УК с введением минимальной суммы ущерба, например более одной базовой величины по аналогии с иными хищениями.

Отдельной проблемой правоприменительной практики рассматриваемых хищений является установление и привлечение к уголовной ответственности лиц, совершивших такие преступления, если они находятся за пределами республики. Как показывает проведенный в 2020 г. анализ этих противоправных действий в Гродненской области около 62 % от всех учтенных преступлений данной категории совершаются в отношении жителей региона из-за пределов Беларуси (преимущественно с территории Российской Федерации и Украины). Практически аналогичная ситуация складывается и в других регионах республики. При этом имеющиеся международные правовые механизмы не позволяют своевременно и в полном объеме получать техническую информацию с использованием возможностей правоохранительных органов иных государств, т. е. существуют объективные трудности по установлению личности преступника и привлечению его к ответственности в соответствии с законодательством Республики Беларусь.

Проблемной является профилактика рассматриваемого вида преступности, особенно из-за низкой компьютерной грамотности населения и несоблюдения элементарных правил «цифровой гигиены». Не секрет, что значительное число профилактических и разъяснительных мероприятий проводятся, как правило, правоохранительными органами, в первую очередь ОВД. К данной работе необходимо привлекать и учреждения образования, органы местной власти и управления, банковские и финансовые учреждения.

Так, по вопросам противодействия хищений путем использования компьютерной техники банковскими учреждениями при взаимодействии с МВД могут быть предприняты следующие меры:

запрет по выдаваемым БПК интернет-платежей с возможностью подключения такой функции по желанию пользователя;

обязательное подключение сервисов дополнительного подтверждения транзакций (3D-Secure, интернет-пароль и т. д.) при возможности интернет-платежей с БПК;

запрет функционирования на территории Республики Беларусь платежных сервисов, не поддерживающих дополнительное подтверждение транзакций;

периодическое информирование банками клиентов о возможных фактах мошенничества посредством размещения такой информации на

сайтах банков, в системах и приложениях интернет-банкинга, а также путем рассылки SMS и push-уведомлений.

Проблему отсутствия в республике единой правоприменительной практики по делам хищений путем использования компьютерной техники, а также других правонарушений, ответственность за которые предусмотрена гл. 31 УК, ввиду различной оценки действий правонарушителей со стороны оперативных сотрудников, следователей, прокуроров и судей возможно решить не только путем изменения законодательства, но и обобщением практики и подготовкой расширенных разъяснений Пленума Верховного Суда Республики Беларусь по вопросам квалификации преступлений, направленных против информационной безопасности.

УДК 343.985

А.В. Изотов

КЛАССИФИКАЦИЯ СПОСОБОВ СОВЕРШЕНИЯ РАЗБОЯ, СОКРЫТИЯ СЛЕДОВ ПРЕСТУПЛЕНИЯ И УКЛОНЕНИЯ ОТ ОТВЕТСТВЕННОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Разработка проблемных вопросов, касающихся способов совершения преступлений, в силу научной и практической значимости являлась и является на современном этапе предметом исследований ученых в сфере криминалистики и оперативно-розыскной деятельности.

Г.Г. Зуйков определяет способ совершения преступления как систему взаимосвязанных и взаимообусловленных действий по подготовке, совершению и сокрытию преступлений, детерминированных условиями внешней среды и свойствами личности, условиями места и времени и нередко связанных с избирательным использованием соответствующих орудий и средств.

В.Ф. Ермолович добавляет, что в содержание данного понятия целесообразно включать такие элементы, как последствия (наступившие, возможные, ожидаемые) совершения преступления; направленность действий, приемов, операций; образ действий преступника; орудия и средства, используемые для сокрытия преступления в целях достижения преступного результата.

В научной литературе имеются отдельные работы, посвященные описанию способов совершения разбоя: связанных как с незаконным проникновением в жилище, так и при нахождении непосредственно в нем