Уголовного кодекса Республики Беларусь, санкция которой предусматривает максимальное наказание до пяти лет лишения свободы, в то время как по санкции ч. 1 ст. 222 УК максимальный срок наказания в виде лишения свободы составляет шесть лет. Как следствие, в такой ситуации изготовление поддельной банковской платежной карточки и ее дальнейшее использование следует квалифицировать лишь как хищение с использованием поддельной банковской платежной карточки, так как использование должно рассматриваться в качестве способа совершения хищения.

Определенные проблемы существуют и в отношении правовой регламентации деяний, связанных с похищением реквизитов банковских платежных карточек. Как правило, на практике для получения данной информации, а также для получения сведений о PIN-коде злоумышленники используют так называемые скиммеры – устройства, предназначенные для копирования информации, содержащейся на магнитной полосе банковской платежной карточки. Причем подобное деяние принято квалифицировать по ст. 352 УК как несанкционированное копирование информации, хранящейся на машинных носителях, повлекшее причинение существенного вреда. Подчеркнем, что причинение существенного вреда является обязательным признаком данного преступления.

Вместе с тем представляется оправданной позиция М.А. Дубко, который ставит под сомнение обоснованность следственно-судебной практики отнесения к общественно опасным последствиям неправомерного завладения компьютерной информацией нарушение вследствие этого правовых предписаний, так как это является, скорее, действием, чем последствием. Например, согласно одному из приговоров несанкционированное копирование лицом информации о реквизитах банковской платежной карточки повлекло за собой причинение существенного вреда, выразившегося в нарушении ст. 28 Конституции Республики Беларусь, т. е. в незаконном вмешательстве в личную жизнь, ст. 121 Банковского кодекса Республики Беларусь, т. е. в несанкционированном получении сведений, составляющих банковскую тайну, а также ст. 17, 18, 27 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», т. е. нарушении конфиденциальности информации о частной жизни физического лица и его персональных данных; нарушении договорных отношений между банками и клиентами.

При этом суд указал, что квалификация деяния, связанного с неправомерным завладением банковской тайной, хранящейся на машинном носителе, с целью совершения последующего хищения (ст. 212 УК), изготовления поддельных банковских платежных карточек (ст. 222 УК) или иного незаконного использования должна осуществляться по совокупности ст. 254 и 352 УК, а при завладении лицом информацией о частной жизни, составляющей личную или семейную тайну другого лица, хранящейся на машинном носителе, квалификация должна осуществляться по совокупности ст. 179 и 352 УК (ввиду особенностей объекта, предмета и признаков объективной стороны составов преступлений конкуренция норм в данном случае отсутствует).

Данный подход к квалификации представляется сомнительным по ряду причин. Прежде всего составы преступлений, предусмотренные ст. 254, 179 УК, а также хищение с использованием банковских платежных карточек либо их реквизитов, помимо отличающихся друг от друга родовых объектов, посягают на общественные отношения, связанные с порядком обращения, доступом к информации. В то же время непосредственным объектом состава преступления, предусмотренного ст. 352 УК, являются общественные отношения, связанные с порядком обращения компьютерной информации.

Под информацией согласно абзацу 12 ст. 1 Закона «Об информации, информатизации и защите информации» следует понимать сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. На основании данного легального определения можно сделать вывод о том, что компьютерная информация – любые сведения, хранящиеся в различных компьютерных системах, в том числе на машинных носителях, поскольку запись информации на них так или иначе связана с определенным программным алгоритмом. Следовательно, банковская тайна, иные сведения о личной жизни могут стать компьютерной информацией, что и вызывает определенную проблему при квалификации. Принимая во внимание объект преступления, при отсутствии доказательств, указывающих на иные нарушения охраняемых общественных отношений, целесообразным представляется квалифицировать завладение реквизитами банковских платежных карточек с учетом положений ч. 2 ст. 42 УК по ст. 352 УК Республики Беларусь при наличии доказательств, указывающих на причинение существенного вреда.

Таким образом, можно сделать вывод о том, что хищение с использованием любых банковских платежных карточек, их реквизитов, помимо отношений собственности, затрагивает отношения, связанные с использованием компьютерной информации. В то же время, поскольку объект посягательства хищения с использованием банковских платежных карточек и их реквизитов охватывает завладение реквизитами, подобные деяния при наличии доказательств, что лицо намеревалось совершить хищение с использованием поддельных банковских платежных карточек, их реквизитов, следует квалифицировать как приготовление к указанному преступлению.

УДК 343

К.В. Диденко

ОБ ОРГАНИЗАЦИИ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВАМ, СОВЕРШАЕМЫМ ДИСТАНЦИОННЫМ СПОСОБОМ

В современном мире достаточно сложно представить свою жизнь без информационно-телекоммуникационных технологий. Они служат базисом национального богатства, способствуют эффективному и динамичному функционированию экономики, выступая системообразующим фактором социальной жизни, и в конечном итоге обеспечивают экономическую, социальную, политическую, военную и другие сегменты безопасности Российской Федерации.

Несмотря на достаточно большое количество положительных аспектов, возникающих при развитии сетей телекоммуникации, следует констатировать ряд негативных процессов, связанных с популяризацией этих технологий, к которым в первую очередь относится высокий уровень криминализации указанной сферы жизни общества. Это достаточно серьезная проблема, так как информационно-телекоммуникационные сети – неотъемлемая часть жизни практически каждого современного человека.

Количество преступлений, совершаемых с использованием информационных технологий, неуклонно растет, методы, способы и средства их совершения становятся все сложнее и изощреннее. Так, в 2019 г. отмечен значительный рост количества преступлений рассматриваемой категории, уголовные дела о которых находились в производстве правоохранительных органов Российской Федерации – 339,3 тыс., что на 64 % превышает показатель предыдущего года (206,8 тыс.), непосредственно за 6 месяцев 2020 г. – 294,4 тыс. (+68,5 % к аналогичному периоду прошлого года, 174,7 тыс.).

В общем количестве зарегистрированных преступлений удельный вес IT-преступлений увеличился с 8,8 % в 2018 г. до 14,5 % в 2019 г.

В массиве уголовных дел данной категории, находившихся в производстве в 2019 г., основную долю (79,1 %) составляют преступления, предусмотренные ст. 158 УК РФ – 110,5 тыс., ст. 159 УК РФ – 137,4 тыс., ст. 159.3 УК РФ – 17,5 тыс., ст. 272 УК РФ – 3 тыс.

Дистанционные мошенничества обладают повышенной общественной опасностью ввиду того, что практически каждый человек пользуется мобильным телефоном либо компьютером и, следовательно, может стать жертвой мошенника. Кроме этого, данный вид преступного посягательства причиняет вред правам, законным интересам личности, а также создает негативное настроение в обществе и подрывает доверие граждан к правоохранительным органам, в частности к органам внутренних дел. Особую актуальность в этой связи приобретает противодействие рассматриваемой категории преступлений.

Анализ практической деятельности сотрудников органов внутренних дел по расследованию уголовных дел указанной категории позволяет выделить следующие способы списания и перечисления денежных средств:

списание денежных средств заявителя, когда неустановленное лицо получает сведения о реквизитах банковской платежной карточки или счета (посредством сети Интернет: «Авито», «Юла», интернет-магазинов и иных торговых площадок);

перечисление денежных средств под предлогом покупки (продажи) товара по сети Интернет («Авито», «ВКонтакте» и т. д.), когда заявитель внес плату (предоплату) за товар, но товар не получил;

перечисление денежных средств под предлогом различных проверок от имени руководителей государственных служб и правоохранительных органов; передачи денежных средств якобы должностным лицом представителю организации либо учреждения; трудоустройства;

перечисление денежных средств под предлогом возврата ранее утерянных документов;

перечисление денежных средств под предлогом разблокировки банковской платежной карточки и предотвращения возможного списания денежных средств;

перечисление (передача) денежных средств под предлогом непривлечения к уголовной ответственности родственников и знакомых потерпевших;

перечисление денежных средств под предлогом возврата денежных средств за ранее приобретенные БАДы (биологически активные добавки), а также оказания помощи экстрасенсами;

перечисление денежных средств под предлогом выдачи кредитов, займов;

перечисление денежных средств, совершенное посредством взлома персональных страниц (аккаунтов) в сети Интернет, в том числе в социальных сетях;

перечисление денежных средств под предлогом проверок различного оборудования (терминалов);

списание денежных средств, совершенное с использованием вредоносных программ (вирусов), получения неправомерного доступа к компьютерной информации, а также иным неустановленным способом списания денежных средств.

Анализ приведенных выше статистических данных, а также способов совершения дистанционных мошенничеств позволили сделать вывод о том, что важное значение в деятельности сотрудников органов внутренних дел должно придаваться профилактике преступности в рассматриваемой сфере, где немаловажную роль имеет информированность населения о видах и способах их совершения.

В этой связи активно используются такие формы работы, как публикации в печатных изданиях, выступления на радио, телевидении, в учебных заведениях и трудовых коллективах.

Следует отметить, что на официальном интернет-сайте МВД России регулярно обновляются памятки для граждан по вопросам предупреждения мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий. Например:

интернет-мошенничество;

советы по определению интернет-ресурсов, несущих потенциальную угрозу финансовому благополучию пользователей;

информация НЦБ Интерпола МВД России о самых распространенных видах мошеннических действий с использованием компьютерных технологий.

В сети Интернет также активно размещаются социальные ролики с названиями: «Как распознать мошенника?», «Осторожно, мошенники», «Мошенники под видом микрофинансовых организаций» и др.

По нашему мнению, для того, чтобы сократить число совершаемых дистанционных мошенничеств, необходимо активное применение профилактических мер. Считаем, что наиболее целесообразна будет профилактика, проводимая в месте совершения преступления – информационном пространстве. В настоящее время существует необходимость разработки системы профилактики дистанционных преступлений в социальных сетях.