мыслительные (когнитивные), эмоциональные, мотивационно-волевые, поведенческие.

Каждая из зон в основном соответствует отдельному виду деятельности следователя, зафиксированному в его профессиограмме.

В соответствии с разработанной технологией может быть предложен следующий алгоритм оперирования данными ресурсами.

1. Предварительно следователю необходимо иметь представление о названных сферах, как о неких базах ресурсов, к которым следует обращаться по мере необходимости. Таким образом, эти хранилища ресурсов (R) будут четырех типов:

мыслительные (когнитивные) – включают ресурсы для логических операций; интуитивной, преобразовательной, творческой работы; мыслительных действий, связанных с восприятием, обработкой, оперированием информацией, ее запоминанием и воспроизведением, а также подобных процессов;

эмоциональные – включают ресурсы по ситуативному эмоциональному совладанию с трудной ситуацией, созданию нужного настроя, мгновенному вхождению в нужное психическое состояние и пр.;

мотивационно-волевые – включают ресурсы, обеспечивающие функциональную готовность независимо от имеющихся препятствий и неблагоприятных условий, а также ресурсы, позволяющие длительное время удерживать необходимую концентрацию внимания, настойчивость, собранность и другие состояния;

поведенческие – включают ресурсы, способствующие совершению оптимальных действий, шагов, операций в процессе расследования преступлений; эти ресурсы способствуют аккуратности, пунктуальности и пр., с точки зрения мысленного контроля над поведением.

2. Поводом для обращения к нужной базе ресурсов должен быть запрос сотрудника, который выражается в осознании конкретного затруднения. Например, если требуется активизировать формулирование новых версий при недостатке доказательственной базы по уголовному делу.

В предлагаемой технологии данный уровень назван «Симптом» (S), так как указывает на соответствующую проблемную область, психологические ресурсы для которой находятся в соответствующей базе ресурсов (R). В данном примере, очевидно – в базе мыслительных (когнитивных) ресурсов.

3. Следующий элемент технологии – «Психотехники» (T), направленные на достижение поставленной цели по разрешению возникшего профессионального затруднения за счет активизации психологического ресурса из соответствующей базы (R). В свою очередь, для решения одной

и той же задачи по устранению конкретного «симптома» (S) может существовать значительное число техник (T). В частности, для приведенного примера может быть использована техника по активизации интуиции.

С использованием данной технологии «Ресурс – Симптом – Техника» (R-S-T) все многообразие психотехник может быть систематизировано по задачам, соответствующим одной из четырех ресурсных баз, и далее следователем может быть использована та из них, которая больше соответствует его наклонностям, имеющемуся времени и которая достаточно доступно описана во многих источниках информации.

Список использованных источников

1. Можаева, И.П. Организация расследования преступлений: правовые, управленческие и криминалистические аспекты / И.П. Можаева // Тр. Акад. упр. МВД России. – М., 2013. – № 4 (28). – С. 78.

2. Долгинов, С.Д. Информационные технологии следственной деятельности / под ред. О.А. Кузнецовой [и др.] // Перм. юрид. альм. Ежегод. науч. журн. ; Перм. гос. нац. исслед. ун-т. – 2018. – № 1. – С. 460–466.

3. Удовиченко, В.С. Научная организация труда дознавателя (следователя) органов внутренних дел : учеб.-метод. пособие / В.С. Удовиченко ; М-во внутр. дел Рос. Федерации, Барнаул. юрид. ин-т. – Барнаул : НИ и РИО БЮИ МВД России, 2014. – 30 с.

4. Белоусов, А.Д. Применение стилевого подхода к описанию интеллектуальной деятельности следователей и дознавателей // Приклад. юрид. психология. – 2018. – № 1 (42). – С. 101–111.

5. Дилтс, Р. Фокусы языка. Изменение убеждений с помощью НЛП / Роберт Дилтс. – СПб. : Питер, 2012. – С. 190–197.

УДК 343

А.В. Вальтер

ДИСТАНЦИОННОЕ МОШЕННИЧЕСТВО В РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКЕ БЕЛАРУСЬ: НЕКОТОРЫЕ АКТУАЛЬНЫЕ ВОПРОСЫ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ

Актуальность темы исследования обусловлена растущим количеством поступающих спам-звонков (вишинг [1]), смс-сообщений на телефонные номера как граждан России, так и Республики Беларусь, целью которых, как правило, является совершение дистанционного электронного мошенничества.

Так, в настоящее время в уголовно-правовой доктрине, принимая во внимание криминалистические знания, отсутствует однозначное мнение относительно понятий о мошеннических действиях, совершаемых удаленным способом с применением телефонной и интернет-связи, не выработана единая научная аббревиатура, исследователи указывают на различные категории преступлений – «IT-преступления», «киберпреступления» и др.

В ходе проведенного анализа отдельных фактов электронного дистанционного мошенничества были выделены общие элементы их совершения: в поисках возможностей совершить хищение денежных средств с банковских счетов граждан большинство поступающих спам-звонков, смс-сообщений совершались с использованием злоумышленниками специальной техники обмана – «социальной инженерии» [2, с. 188–210], – которая в настоящее время достаточно исследована. Весомую роль, полагаем, занимают откровения о технологиях обмана, изложенные в исследованиях бывшего хакера, а в настоящее время эксперта по компьютерной безопасности в США Кевина Дэвида Митника, «Искусство обмана» [3].

Страхи в виде потери денежных средств, хранящихся на банковском счете, в совокупности с имеющимися новейшими возможностями дистанционного контроля потерпевшего и использованием специального программного обеспечения, интернет- и телефонного соединения представляют для мошенников в настоящее время практически безграничные возможности в ходе совершения преступной деятельности, связанной с дистанционным электронным мошенничеством.

Так, с целью дальнейшей алгоритмизации проведения следственных действий по уголовным делам, предусмотренным ст. 159, 159.3, 159.6 УК Российской Федерации, совершенным бесконтактным способом, необходимо создание единой уголовно-правовой концепции в виде отдельной категории преступлений, именуемой дистанционное электронное мошенничество. Так, В.Г. Любан в своем исследовании 2019 г. использовал термин «дистанционное мошенничество» [4, с. 66–69], однако по настоящее время данный термин не был раскрыт в полном объеме.

По нашему мнению, именно дистанционное электронное мошенничество – это хищение имущества в виде безналичных денежных средств и (или) электронных денежных средств с использованием электронных средств платежа, в совокупности с технологиями обмана, информационно-телекоммуникационным или телефонным способом.

Анализируя уголовное законодательство Республики Беларусь, представляется, что факты электронного дистанционного мошенничества рассматриваются в аспекте ст. 209 «Мошенничество» УК Республики Беларусь.

Так, например, следователь, используя общедоступные базы данных, может инициативно установить первоначальную информацию для дальнейшего направления запросов в соответствующие коммерческие организации, предоставляющие различные цифровые услуги (провайдеры сотовой связи и интернета, IP-телефония, услуги доменных имен, хостингов и др.).

Приведем пример одного из распространенных способов дистанционного электронного мошенничества, при котором на телефон потерпевшего поступает спам-звонок с целью получить конфиденциальную информацию о банковском счете, после чего последний сообщает злоумышленнику всю необходимую информацию о своем банковском счете, банковской платежной карточке, пин-коды и преступник распоряжается похищенными безналичными денежными средствами. В данном аспекте возникают определенные сложности временного характера, т. е. вопросы охраны конфиденциальных данных банковских счетов клиентов, когда в силу вступает законодательство в области банковской деятельности, охраняющей тайну лиц, осуществляющих открытие счетов, платежей и другие операции в кредитно-финансовой сфере [5, 6]. В связи с чем, полагаем, целесообразно с целью сокращения времени для установления первоначальной информации, имеющей доказательственное значение по уголовному делу, получение потерпевшим инициативно выписки по банковскому счету (с которого у лица совершили хищение безналичных денежных средств) и передачей данной информации следователю, а также в кратчайшие сроки получение развернутой информации от оператора сотовой связи, на котором зарегистрирован абонентский номер, о поступившем звонке от злоумышленника. Необходимо также учитывать, что в настоящее время могут использоваться различные уловки с применением Voice over IP-телефонии и искусственного изменения входящего номера телефона с целью войти в доверие к жертве (спуфинг) [7, с. 928].

Следователь также имеет возможность самостоятельно установить предварительную информацию об актуальном операторе связи, смене оператора связи, смене абонентского номера телефона злоумышленника, используемом устройстве (телефон, планшет, компьютер и др.) путем использования программных средств, представленных на интернет-сайтах www.zniis.ru, www.htmlweb.ru и др., и осуществить впоследствии направление запросов актуальным операторам связи, представляющим в том числе услуги Интернет-телефонии.

Так, в связи с поступившими в наш адрес телефонных спам-звонков от оператора колл-центра банка, которая сослалась на некие финансовые операции, проведенные с использованием банковской платежной карточки, и попыталась с использованием технологии «социальной ин-

женерии» установить конфиденциальную информацию о банковских счете, платежной карточке. В ходе проведенного эксперимента была осуществлена проверка по открытым источникам баз данных в отношении абонентского номера звонившего абонента (по входящему номеру телефона): 8 (495) 201 XX XX и установлено, что телефон зарегистрирован оператором связи ЗАО (АО) «Кантри….» (г. Москва, 127018, проезд Марьиной Рощи…., генеральный директор – И.С.И.). Таким образом, в ходе проведенных технических манипуляций был инициативно установлен оператор связи и иная значимая информация.

В ином случае использовались спам-рассылки: «Не смогла до Вас дозвониться. На Ваши Ф.И.О. истекает срок получения денежной компенсации. Получите на сайте http://www.compensacia.online». В ходе проведенной проверки установлено, что сайт зарегистрирован 13 февраля 2021 г., registrar URL – www.name...com, registrant organization: PrivacyGuardian.org (США, штат Аризона), контакты для связи с организациями, имеющими отношение к регистрации доменного имени: abuse@name...com, телефон: +1.480524XXXX.

Приведенные примеры – это лишь часть имеющихся проблем в ходе расследования фактов дистанционного электронного мошенничества, так как в дальнейшем возникают сложности в рамках международного взаимодействия и иных ограничений в ходе поиска цифровых следов преступления (VPN-шифраторы IP-адресов, использование подложных паспортных и иных данных при регистрации домена, использование зарубежных хостинг-ресурсов, оплата за услуги интернет- и мобильной связи сторонними лицами и др.).

Проведенный мини-эксперимент позволил показать, что возможно оперативно получить первоначальную информацию о цифровых следах преступления [8, с. 4–19] для построения следственных версий по оставленным злоумышленниками цифровым следам в ходе спам-прозвона, смс-сообщений, регистрации спам-сайтов и фактам оплаты за абонентские номера и иные телекоммуникационные ресурсы.

Список использованных источников

1. Следы телефонного мошенничества с банковскими картами ведут в Россию и Украину [Электронный ресурс] / Белта-Новости Беларуси. – Режим доступа: https://www.belta.by/incident/view/sledy-telefonnogo-moshennichestva-s-bankovskimi-kartami-vedut-v-rossiju-i-ukrainu-mvd-370833-2019. – Дата доступа: 12.03.2021.

2. Грачева, Ю.В. Предупреждение девиаций в цифровом мире уголовно-правовыми средствами / Ю.В. Грачева, С.В. Маликов, А.И. Чучаев // Право. Журнал Высш. шк. экономики. – 2020. – № 1. – С. 188–210.

3. Mitnick Kevin, W.l. Simon The art of deception. – 2002.

4. Любан, В.Г. Правовой анализ практики направления по территориальной подследственности материалов доследственной проверки с признаками дистанционных хищений безналичных денежных средств / В.Г. Любан // Рос. юстиция. – 2019. – № 5. – С. 66–69.

5. Банковский кодекс Республики Беларусь [Электронный ресурс] : 25 окт. 2000 г., № 441-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

6. О банках и банковской деятельности [Электронный ресурс] : Федер. закон, 2 дек. 1990 г., № 395-1 : в ред. от 30.12.2020 г. // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2021.

7. Кондрат, Е.Н. Правонарушения в финансовой сфере России. Угрозы финансовой безопасности и пути противодействия / Е.Н. Кондрат. – М. : Юстицинформ, 2014. – 928 с.

8. Доминик, Б. Цифровые доказательства в немецком уголовном процессе на стадиях предварительного расследования, рассмотрения дела по существу и ревизии / Б. Доминик, Я. Маттиас // Рос. право: образование, практика, наука. – 2020. – № 3. – С. 4–19.

УДК 343.98

Д.Г. Вильмак

ОСОБЕННОСТИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА ПО ФАКТУ НЕЗАКОННОЙ ДОБЫЧИ РЫБЫ

Традиционно этап возбуждения уголовного дела анализируют как своеобразный фильтр уголовного судопроизводства. Мы согласны с суждением ученых, считающих, что собственно с этой позиции данная стадия уголовного процесса и остается в законодательстве, обязывая правоприменителя принимать нужные меры к скрупулезной проверке сведений о правонарушении, с тем, чтобы не допустить приведения в действие всего механизма уголовного судопроизводства напрасно [1, с. 27–31].

После возбуждения уголовного дела следователь начинает проведение процессуальных действий, которые направлены на раскрытие и расследование конкретного правонарушения или в отношении конкретного лица. От скорого и верного решения вопроса о возбуждении уголовного дела во многом зависит его успешное расследование с дальнейшим направлением в суд.

В соответствии с действующим уголовно-процессуальным законодательством Республики Беларусь и Российской Федерации для принятия решения о возбуждении уголовного дела необходимо убедиться в при-