ная ответственность за несанкционированный доступ к компьютерной информации предусмотрена ст. 349 УК Республики Беларусь.

Сам доступ можно считать несанкционированным с момента получения злоумышленником возможности присвоения информации и пользования ею по своему усмотрению и без разрешения пользователя. Обязательным признаком объективной стороны несанкционированного доступа к компьютерной информации является нарушение систем защиты, которое рассматривается как способ совершения преступления, указанного в ст. 349 УК. Нарушение систем защиты в большинстве случаев осуществляется с применением программно-технических средств (вредоносных программ).

Был проведен сравнительный анализ статей УК. Отмечено следующее.

Вымогательство с объективной стороны характеризуется требованием передачи имущества или права на имущество под угрозой применения насилия к потерпевшему или его близким, уничтожения или повреждения имущества, распространения клеветнических сведений или оглашения иных сведений, которые они желают сохранить в тайне (ч. 1 ст. 208 УК). Если вымогательству предшествует несанкционированный доступ к компьютерной информации, когда злоумышленники нарушают систему защиты и от лица другого человека требуют передать имущество, подобные действия образуют совокупность преступлений и квалифицируются по ст. 208 и 349 УК.

Мошенничество с объективной стороны характеризуется завладением имущества или приобретением права на имущество путем обмана или злоупотребления доверием (ч. 1 ст. 209 УК). Несколько лет назад были распространены случаи следующего мошенничества: злоумышленник получал несанкционированный доступ к социальным сетям и, выставляя себя за другого человека, путем обмана завладевал чужим имуществом. Данные действия также образуют совокупность преступлений и квалифицируются по ст. 209 и 349 УК.

Объективная сторона хищения путем использования компьютерной техники (ст. 212 УК) характеризуется хищением имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации. При этом за хищение имущества путем использования компьютерной техники, сопряженное с несанкционированным доступом к компьютерной информации, по ч. 2 ст. 212 УК предусмотрена ответственность. Таким образом, исходя из ч. 2 ст. 212 УК, несанкционированный доступ к компьютерной информации выступает в качестве способа совершения анализируемого преступления. При возникновении проблемы отграничения ч. 2 ст. 212 УК от ст. 349 УК мы можем говорить о конкуренции части и целого, при которой применению подлежит норма, наиболее полно охватывающая совершенное преступление. Следовательно, применению подлежит ч. 2 ст. 212 УК и дополнительной квалификации по ст. 349 УК не требуется.

В преступлениях, указанных в ст. 350 (модификация компьютерной техники) и 351 (компьютерный саботаж) УК, несанкционированный доступ к компьютерной информации выступает в качестве квалифицирующего признака, и дополнительная квалификация не требуется.

Исходя из анализа ст. 208, 209, 212, 350 и 351 УК, следует отметить, что в настоящее время преступления, которые совершаются при помощи компьютерных систем, прямо или косвенно связаны с несанкционированным доступом к компьютерной информации.

Одними из наиболее эффективных методов решения проблемы квалификации и правоприменения норм ст. 349 УК являются опубликование подробного толкования законодателем норм гл. 31 УК и распространение судебной практики по делам, связанным с несанкционированным доступом к компьютерной информации.

УДК 343.8

С.И. Давыдов, Е.О. Наливайко

О ФОРМИРОВАНИИ ОПЕРАТИВНО-РОЗЫСКНОЙ ХАРАКТЕРИСТИКИ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

В начальный период формирования теории оперативно-розыскной деятельности проблему понятия оперативно-розыскной характеристики (ОРХ) преступлений рассматривали в своих работах А.И. Алексеев, В.М. Атмажитов, В.Г. Бобров, В.В. Гордиенко, Ю.В. Дамов, Б.П. Смагоринский, Л.Л. Тузов, В.Б. Утевский, Ю.М. Худяков, А.Ю. Шумилов и другие известные ученые.

Свое развитие учение об ОРХ преступлений получает и в настоящее время, о чем свидетельствует целый ряд публикаций (авторы Б.В. Борин, П.И. Иванов, В.Ф. Луговик, В.Н. Омелин, Д.Ю. Федорович, А.И. Хмыз и др.). Некоторые из них посвящены специально ОРХ дистанционного мошенничества (авторы В.Г. Горбанев, В.Г. Любан, А.Ю. Молянов, Е.Н. Хазов, А.П. Подшивалов, А.С. Малахов и др.).

Анализ научной литературы позволяет выделить два принципиальных подхода к определению понятия ОРХ преступлений. Первый под-

ход основан на описании с разной степенью детализации элементов ОРХ преступлений. Нам более привлекателен другой подход: ученые абстрагируются от детализации структуры ОРХ и определяют ее понятие, раскрывая ее сущность, познавательные функции и целевое значение.

При определении понятия и содержания ОРХ дистанционного мошенничества весьма полезно обратиться к фундаментальным криминалистическим исследованиям проблемы криминалистической характеристики преступлений (авторы Р.С. Белкин, А.В. Васильев, В.К. Гавло, В.Я. Колдин, Н.П. Яблоков и др.). Из числа последующих исследований выделим труды И.И. Рубцова, А.С. Князькова, А.А. Бессонова.

На основе анализа научных источников приходим к следующему определению ОРХ дистанционного мошенничества. ОРХ дистанционного мошенничества – совокупность наиболее характерной оперативно значимой взаимосвязанной информации о признаках его подготовки, совершения и сокрытия, имеющей значение для формирования частной методики раскрытия дистанционных мошенничеств и определяющей содержание практической деятельности оперативных подразделений по их раскрытию.

Представляется, что вопрос определения структурных элементов ОРХ дистанционного мошенничества следует решать исходя из ряда общих положений, сформулированных в разное время в оперативно-розыскной теории. Таковыми являются следующие положения:

в систему ОРХ должны входить обобщенные данные о наиболее типичных, устойчивых и повторяющихся оперативно значимых признаках преступления;

количество и содержание образующих ОРХ элементов не могут быть универсальными: они определяются конкретным видом (группой) преступлений, поскольку элементы, информативные в оперативно-розыскном отношении для одних групп преступлений, могут быть неинформативными или слабо информативными для других групп (идею о главных и факультативных признаках ОРХ преступлений развивает, в частности, в своих трудах В.Ф. Луговик);

для разработчиков частных оперативно-розыскных методик и практических сотрудников важны сведения о наличии корреляционных связей между элементами ОРХ, которые, как пишет А.А. Бессонов применительно к криминалистической характеристике, могут быть двух видов: корреляционные (однозначные), при которых наличие одного элемента позволяет совершенно определенно судить о существовании другого, а изменение характеристики первого из элементов влечет изменение характеристики второго; вероятностно-статистические, при которых установление одного элемента позволяет с большей или меньшей степенью вероятности предполагать наличие другого элемента;

при разработке ОРХ преступлений целесообразно использовать достижения других наук в области исследования преступности – уголовного права, криминологии, криминалистики, а также юридической психологии, учитывая, что каждая наука изучает лишь те аспекты преступления, которые значимы для решения стоящих перед ней теоретических и практических задач;

ОРХ преступлений должна включать в себя такие данные, которые определяют содержание организации, тактики деятельности оперативных подразделений по выявлению, раскрытию преступлений оперативно-розыскными средствами и методами, преимущественно негласными.

Если проанализировать труды ученых в области ОРД, в которых исследуются элементы ОРХ преступлений, можно выделить ряд таких элементов: они упоминаются наиболее часто и обладают достаточной степенью информативности для большинства видов (групп) преступлений. Этими элементами являются данные: о личности преступника; обстановке совершения преступления; механизме следообразования; способах подготовки, совершения преступления и противодействия его раскрытию; предмете преступного посягательства и (или) личности потерпевшего. Данный перечень, конечно, не является исчерпывающим, но может быть основополагающим для определения элементов ОРХ дистанционного мошенничества. К тому же, с нашей точки зрения, в ОРХ преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, необходимо выделять такой ее элемент, как характеристика средств их совершения (сеть Интернет, сотовая связь) и электронных носителей информации.

Для определения содержания ОРХ дистанционного мошенничества, отметим, важны те ее элементы, которые необходимы для достижения цели разработки эффективных мер по организации деятельности оперативных подразделений по выявлению и раскрытию указанных преступлений. Критерии отбора элементов ОРХ дистанционного мошенничества следующие: их закономерная повторяемость (устойчивость), научная обоснованность, измеримость и формализуемость, предназначенность для организации деятельности оперативных подразделений по раскрытию указанных преступлений.

С учетом изложенного считаем, что наиболее важными структурными элементами ОРХ дистанционного мошенничества являются оперативно значимые данные:

о динамике, распространенности, результатах их раскрываемости;

обстановке их совершения;

способах подготовки, совершения и сокрытия дистанционного мошенничества (способы обмана потерпевших, приемы манипуляций их сознанием и поведением);

особенностях личности преступника;

информационно-коммуникационной среде как сфере возникновения информации о совершении дистанционных мошенничеств;

механизме образования следов как источников информации о дистанционных мошенничествах;

видах электронных носителей информации об обстоятельствах дистанционных мошенничеств.

Задача исследователей – наполнение каждого из элементов ОРХ дистанционного мошенничества своим содержанием на основе изучения материалов оперативно-следственной и судебной практики.

УДК 343.98

В.М. Данатарова

СОВРЕМЕННЫЕ СПОСОБЫ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОЙ СВЯЗИ

В связи с интенсивным развитием средств мобильной связи, технологическими прорывами в сфере мобильных гаджетов, а также в связи с формированием привязанности к ним возрастает количество мошенничеств, совершенных с их использованием.

Изучая научные работы, посвященные мошенничеству с использованием мобильной связи, мы приходим к выводу, что исследования в данном направлении практически отсутствуют или имеют поверхностный характер.

В большинстве научных работ описаны основные виды мошенничества: «получите выигрыш», «нигерийские письма», «ваш родственник в полиции», «ошибочное пополнение мобильного счета», «звонок из банка» и т. п. Они уже являются достаточно изученными со стороны ученых, не вызывают у практиков трудностей в их раскрытии и используются преступниками крайне редко.

Мы считаем, что необходимо уделить внимание относительно новым видам мошенничества и рассмотреть их способы совершения, с которыми на сегодняшний день сталкиваются и испытывают трудности сотрудники подразделений по борьбе с киберпреступностью МВД Украины.

Так, одним из современных способов завладения денежными средствами жертвы является SMS-фишинг. В декабре 2020 г. одним из фи-

нансовых учреждений Украины были зафиксированы рассылки фишинговых SMS-сообщений с использованием поддельных альфа-имен банков. Прежде всего стоит разобраться, что же такое альфа-имя. Согласно информации указанной в словаре терминов, альфанумерическое имя, или альфа-имя, – 11 символов в строке отправителя SMS. В нем указывается название компании или бренда, но не номер мобильного телефона. Например, банковское учреждение «Кредобанк» при SMS-рассылке использует альфа-имя KREDOBANK (состоит из больших букв латиницы). Мошенники подделывают такие альфа-имена банков, чтобы вызвать доверие у клиентов финансовых учреждений.

Используя поддельное альфа-имя, мошенники совершают рассылку сообщений, в которых описаны вымышленные проблемы с платежной картой потенциальной жертвы (блокировка платежной карты, кража данных платежной карты и т. п.) и одним из способов решения проблемы предлагается немедленно связаться с сотрудником банка и следовать его указаниям. Целью такого SMS-сообщения является создание информационно-психологического влияния для умышленного введения пользователя в заблуждение. Находясь в состоянии стресса, взволнованная жертва следует указаниям лже-сотрудника банка – совершает выведение денежных средств путем перечисления на «безопасный» счет, уже якобы открытый учреждением на имя клиента. Таким образом, потерпевший, находясь под влиянием мошенника, с целью защиты своих денежных средств выполняет манипуляции по перечислению денег прямо на счет преступника.

Мошенники, использующие SMS-фишинг, могут представляться сотрудниками банков, сервисных компаний или компаний-операторов лотерей. Как показывает практика, аргументы в их арсенале могут быть разные, но задача состоит в том, чтобы непосредственно выманить денежные средства и получить доступ к управлению текущим счетом.

Сходным способом пользуются преступники и для создания условий кражи авторизационных данных для доступа к системам дистанционного банковского обслуживания (онлайн-банкинга) и платежных карточек. Но стоит отметить, что в этом случае денежные средства похищаются втайне от потерпевшего. Посему имеет место квалификация такого преступления как кража (тайное хищение чужого имущества).

Следующим способом совершения мошенничества является использование чат-ботов. Чат-бот (англ. chatbot) – программа, которая имитирует реальный разговор с пользователем. Чат-боты позволяют общаться с помощью текстовых или аудиосообщений на сайтах, в мессенджерах, мобильных приложениях или по телефону. Согласно информации на