При проведении оперативно-розыскных мероприятий по установлению лица, совершившего киберпреступление, могут возникнуть несколько препятствий.

Анонимность – одно из таких препятствий. Она позволяет людям участвовать в деятельности, не раскрывая себя и (или) свои действия другим. Анонимность предоставляют пользователям информационные и коммуникационные технологии. Есть несколько способов анонимизации, один из которых основан на использований прокси-сервера. Прокси-сервер – промежуточный сервер, поскольку он используется для подключения к серверу клиента, т. е. его компьютера, который запрашивает ресурсы. Анонимайзеры, или анонимные прокси-серверы, скрывают идентификационную информацию пользователей, маскируя их IP-адреса и заменяя их другим IP-адресом. Киберпреступники также могут использовать анонимные сети для шифрования трафика и сокрытия адреса интернет-протокола или IP-адреса (уникального идентификатора), присвоенного интернет-провайдером компьютеру или другому цифровому устройству, подключенному к сети. В этих анонимных сетях не только маскируются данные о пользователях, но и размещаются вебсайты, доступные только пользователям этих сетей.

Атрибуция – еще одно препятствие, с которым сталкиваются сотрудники правоохранительных органов при раскрытии киберпреступлений. Она закрепляется в определении, кто или что несет ответственность за совершение киберпреступления. Однако киберпреступность пытается этот процесс подменить, приписав конкретному цифровому устройству, пользователю устройства или другим лицам ответственность за совершение киберпреступления. Использование инструментов анонимности может затруднить идентификацию устройств и лиц, совершивших киберпреступление. Атрибуция дополнительно осложняется использованием зараженных вредоносным программным обеспечением бот-компьютеров или бот-сетей либо цифровых устройств, управляемых без ведома пользователя инструментами удаленного доступа, для совершения киберпреступлений.

Третьим препятствием раскрытию киберпреступлений является обратное отслеживание – процесс отслеживания незаконных действий до их источника, т. е. преступника или цифрового устройства. Отслеживание проводится после того, как киберпреступление произошло либо было обнаружено, для выявления информации путем изучения всех обстоятельств происшедшего, а также компьютерных устройств, которые могут раскрыть информацию о киберпреступлении. Например, изучаются журналы событий операционной системы Windows, которые автоматически записывают события, происходящие на компьютере, чтобы

в дальнейшем данные сведения можно использовать для мониторинга, понимания и диагностики действий и проблем в компьютерной системе. Такими являются журналы приложений, которые записывают события, регистрируемые программами (приложениями), и журналы безопасности, в которых записываются все попытки входа в систему, как действительные, так и недействительные, а также создание, открытие или удаление файлов, программ или других объектов. Время, необходимое для завершения процесса обратного отслеживания, зависит от знаний, навыков и возможностей киберпреступников, а также от тактики, которую они используют для участия в противоправной деятельности.

Таким образом, в настоящее время правоохранительные органы многих стран, в том числе и Республики Беларусь, сталкиваются с серьезными проблемами при раскрытии киберпреступлений. Для устранения описанных препятствий при раскрытии киберпреступлений необходимо активно применять профилактические меры по отношению к пользователям компьютерных сетей, использовать новейшее специализированное программное обеспечение для анализа полученной информации, а также регулярно повышать квалификации сотрудников правоохранительных органов, занимающихся раскрытием киберпреступлений.

УДК 343.985

Е.И. Давидович, Д.А. Новаш

СВЯЗЬ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ СО СМЕЖНЫМИ СОСТАВАМИ ПРЕСТУПЛЕНИЯ

В конце XX в. большая часть информации была размещена в цифровом пространстве. В условиях активного развития информационных технологий большинство преступлений видоизменились и противоправные замыслы стали реализовываться с помощью компьютерных систем, в результате чего возникла проблема корректной реализации норм права и правильной квалификации преступлений, связанных с несанкционированным доступом к компьютерной информации. Решение данной проблемы должно способствовать реализации принципа законности и правильной квалификации преступлений.

Несанкционированный доступ к компьютерной информации – неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающееся нарушением систем защиты лицом, которое не имеет на это права. Уголов-

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-