УДК 343.98.06

ТИПИЧНЫЕ СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ОБСТАНОВКИ КИБЕРПРОСТРАНСТВА

Елена САМОЙЛЕНКО,
кандидат юридических наук, доцент,
доцент кафедры криминалистики
Национального университета «Одесская юридическая академия»

АННОТАЦИЯ

В статье осуществляется типизация способов совершения традиционных преступлений с использованием обстановки киберпространства. В результате анализа материалов практики выделено восемь групп типичных для Украины способов совершения таких преступлений. Избрание злоумышленником определенной из компьютерных технологий за основу своей преступной деятельности послужило основанием для классификации способов исследуемых преступных действий. В частности, выделены способы преступных действий, связанные с функционированием следующих технологий: 1) социально ориентированных сетей; 2) BitTorrent; 3) сервисов электронной доски объявлений; 4) электронной коммерции; 5) электронной рассылки, IP-телефонии; 6) электронных платежных систем; 7) сохранения и обработки информации; 8) вредоносного программного обеспечения.

Ключевые слова: киберпространство, пользователь, преступление, преступник, способы, технологии.

TYPICAL WAYS OF PREVENTING CRIMES RELATED TO USE OF THE CYBERSPACE SPACE

Elena SAMOYLENKO,
Candidate of Law Sciences, Associate Professor,
Associate Professor of the Department of Criminalistics
of National University "Odessa Law Academy"

SUMMARY

The article typifies the ways of committing traditional crimes using the environment of cyberspace. As a result of the analysis of the materials of the practice, eight groups of typical ways for Ukraine to commit such crimes were identified. The choice by an attacker of a certain computer technology as the basis of his criminal activity served as the basis for classifying the methods of the criminal activities investigated. In particular, the methods of criminal actions related to the functioning of the following technologies are identified: 1) socially-oriented networks; 2) BitTorrent; 3) electronic bulletin board services; 4) e-commerce; 5) electronic mailing, IP-telephony; 6) electronic payment systems; 7) preservation and processing of information; 8) malicious software.

Key words: cyberspace, user, crime, criminal, ways, technologies.

Постановка проблемы. Любой процесс преступной деятельности, который предполагает использование киберпространства, с течением времени технологически усложняется. Закономерное усовершенствование компьютерных технологий приводит к появлению новых способов совершения преступлений, связанных с использованием обстановки киберпространства.

Актуальность темы исследования. Способы совершения преступлений с использованием обстановки киберпространства как самостоятельная категория являются малоисследованными в криминалистической науке.

Состояние исследования. В.В. Крылов, О.П. Снегирев, О.В. Голубев, Ю.М. Батурин, В.Б. Вехов и другие ученые в своих работах описывали способы совершения сугубо компьютерных преступлений. Осуществляли они это путем разнообразных классификаций способов совершения преступлений, в частности: по виду компьютерного преступления, по типу компьютерной защиты, по методу выполнения преступником тех или других действий, направленных на получение доступа к средствам компьютерной техники [1–3]. Ученые часто прибегают к детализации отдельных способов, предложенных в кодификаторе компьютерных преступлений Генерального Секретариата Интерпола, используя при этом специальную техническую терминологию. Однако следует подчеркнуть, что типизация способов совершения любого вида преступлений базируется на эмпирических данных с последующим переходом к их аналитической обработке. Анализ судебно-следственной практики позволяет утверждать, что в описательной части процессуальных документов по делам исследуемой категории (в части описания фабулы события преступления) всегда содержится указание на информационно-коммуникационные технологии, которые позволили достичь преступного результата. Поэтому, по нашему убеждению, в классификации способов совершения преступлений с использованием обстановки киберпространства необходимо учитывать не только фактический способ действий преступника, но и информационно-коммуникационные технологии, что были положены в основу достижения конечной преступной цели.

Целью статьи является типизация способов совершения традиционных преступлений с использованием обстановки киберпространства.

Изложение основного материала. С.В. Кригин, рассматривая модель

преступления в сфере компьютерной информации в контексте способов его совершения, предлагает описывать типичную систему признаков по отношению к каждому отдельно взятому способу. В целом достаточно осложняя описание способов совершения преступления, автор справедливо акцентирует на том, что субъект выявления и расследования преступления должен иметь знание о технологиях обработки информации, которые использует преступник [4, с. 86]. Именно в этом есть смысл с позиций совершения преступлений с использованием обстановки киберпространства.

Д.Г. Цехан отмечает, что качественное усовершенствование способов совершения традиционных преступлений приводит к появлению своеобразных технологий преступной деятельности. Это дает право автору писать о наличии корреляционных связей между высокими информационными технологиями и инновационными формами преступной деятельности [5, с. 43]. По нашему мнению, именно информационно-телекоммуникационные технологии выполняют функцию элемента, обеспечивающего интерактивное взаимодействие способа и технологии совершения преступлений исследуемой категории, ведь они свойственны как способам, так и технологиям совершения таких преступлений.

В ст. 1 Закона Украины «О Национальной программе информатизации» информационная технология определена как организованная совокупность информационных процессов с использованием средств вычислительной техники, что обеспечивают высокую скорость обработки данных, быстрый поиск информации, рассредоточение данных, доступ к источникам информации независимо от места их расположения [6]. Поскольку все эти процессы в настоящее время происходят посредством средств компьютерной техники, уместным представляется применение и других терминов, в частности «компьютерно-информационные технологии» или «кибертехнологии». Особенную научную ценность для исследования способов совершения преступлений с использованием обстановки киберпространства имеет классификация таких технологий в зависимости от сфер их применения на две большие группы [7]: а) базовые (универсальные) технологии – их используют практически во всех сферах деятельности; б) технологии предметных отраслей (специальные) – их применяют в определенных сферах деятельности субъекта. Специалисты по информатики делят базовые технологии на группы в зависимости от видов обрабатываемой информации: 1) для обработки разных данных – система управления базами данных и табличные процессоры; 2) для обработки текста – текстовые процессоры, технологии гипертекстовой связи документов; 3) для обработки графики – графические процессоры; 4) для обработки объектов реального мира – средства мультимедиа. Название «технологии предметных отраслей», или «специальные технологии» свидетельствует сама за себя. Такие технологии разделяют на подгруппы в зависимости от сфер их применения, например, существуют технологии электронной коммерции, технологии электронного документооборота, банковские технологии, экспертные системы, вредоносное программное обеспечение, блокчейн-технология (с англ. «blockchain», для обращения криптовалюты Bitcoin), технологии робототехники, технологии умного дома и тому подобное.

Считаем, что избрание злоумышленником определенной из компьютерных технологий за основу своей преступной деятельности может послужить основанием для классификации способов преступных действий с использованием обстановки киберпространства. В результате анализа материалов следственно-судебной практики типичные сегодня в Украине способы совершения преступлений с использованием обстановки киберпространства можно классифицировать следующим образом.

1. Способы преступных действий, связанные с функционированием социально ориентированных сетей (от англ. social networks), деятельность которых основана на так называемой viki-технологии. Последняя является технологией построения Web-системы, предназначенной для коллективной разработки, сохранения, структуризации текста, гипертекста, файлов, мультимедиа. Пользователь получает возможность зарегистрироваться и размещать на своей интернет-странице (аккаунт) любую информацию о себе, свои интересы, события из личной и общественной жизни, обсуждать (в онлайн или офлайн режимах) с другими пользователями сети любые темы [8, с. 159-162]. Обычно преступник начального уровня и уровня пользователя с целью доведения к сведению неограниченного количества пользователей социальной сети, а также извещения всех пользователей сети, которые прибавлены к разделу «Друзья» этого аккаунта, размещает (из собственного компьютера или осуществляет так называемый «репост» – распространение с другого электронного источника) на странице фото-, видеофайлы, другие формы публикации противозаконного характера, которые содержат: порнографию (часто детскую); призывы к насильственному изменению конституционного строя, изменению границ территории и государственной границы Украины, к совершению террористического акта; пропаганду культа насилия и жестокости, расовой, национальной и религиозной нетерпимости, войны, коммунистического и нацистского тоталитарных режимов; информацию направляющего (мотивирующего) характера на совершение террористических актов (тем самым осуществляется вербовка людей), на трудоустройство молодых женщин за границу, самоубийства; распутные действия интеллектуального характера относительно малолетнего или несовершеннолетнего лица.

Способы подготовки связаны с загрузкой, поиском, созданием, сохранением, редактированием соответствующих текстовых, фото-, видеофайлов или других форм публикации. Способы сокрытия чаще всего отсутствуют. В отдельных случаях для обеспечения анонимности преступник может использовать виртуальные частные сети (VPN-технологии). Приведенная группа способов преступления может реализовываться в форме единичного преступления или содержать много эпизодов преступной деятельности. Многоэпизодная преступная деятельность может иметь долговременный характер, что сегодня достаточно характерно. Так, с 2012 до 2016 года житель Кировограда гр. П. размещал в созданном им аккаунте призывы

к изменению границ территории Украины, что было квалифицировано как посягательство на ее территориальную целостность [9].

2. Способы преступных действий, связанные с функционированием технологии BitTorrent, созданной для передачи больших по объему файлов одним пользователем другому или общественности. Преступники-пользователи удачно применяют эту технологию для распространения через Интернет компьютерных программ, аудиовизуальных произведений, баз данных (компиляции данных), фонограмм и организации вещания с нарушением авторского или смежных прав путем их размещения для копирования в сети, а также произведений, имеющих порнографический характер, путем предоставления доступа к ним пользователям. Так, житель города Запорожье в период с 30 августа до 21 сентября 2012 года, совершил распространение видеофайлов порнографического содержания, с использованием интернет-ресурса «tracker.zp.ua» [10].

3. Способы преступных действий, связанные с функционированием сервисов электронной доски объявлений (от англ. аббревиатуры «*BBC*»). Наиболее распространенными досками объявлений являются сервисы, которые действуют в режиме онлайн связи, – украинцы часто используют «olx.ua», «bigl.ua» (ранее «aykro»), «ria.com», а также соответствующие заграничные сервисы.

В настоящее время мошеннические действия массово совершаются путем размещения объявления относительно продажи пользователям любого материального предмета, причем преступник не намеревается поставлять его покупателю. Злоумышленник заверяет пострадавшего, что отправит заказанный товар курьерской/почтовой службой по получении им как предоплаты денежных средств, для чего используются возможности разнообразных платежных систем и сервисов Интернет-банкинга. Так, житель г. Никополь, пользуясь сайтом «olx.ua», многократно совершал аналогичные мошеннические действия, предлагая пострадавшим приобрести двухколёсный скутер. Жертвы с использованием Интернет-банкинга «Приват24» осуществляли оплату товара [11].

Также преступник, разместив объявление, может быть продавцом оружия, боевых припасов или взрывчатых веществ, наркотических средств, психотропных веществ или их аналогов и прекурсоров, специальных технических средств получения информации. Так, в первой декаде ноября 2016 года житель г. Ровно посредством сайта электронной торговли «AliExpress» приобрел в КНР специальные технические средства негласного получения информации (а именно GSM-микрофоны). Убедившись, что они в рабочем состоянии и пригодные для использования по назначению, злоумышленник незаконно сбыл их разным гражданам с использованием сети Интернет посредством сайтов «Olx», «Ukgro», «Evende» и «Weebly» через отделение «Новой почты» при условиях «наложенного платежа» [12].

4. *Способы преступных действий, связанные с функционированием технологий электронной коммерции, созданные с осуществлением торговли через Интернет.* Термином «технологии электронной коммерции» обозначают разнообразные принципы, которым должно отвечать программное обеспечение и сервисы для электронной коммерции. На основании анализа материалов уголовных производств можно назвать такие распространенные группы способов преступных действий с использованием технологий электронной коммерции.

4.1. Заказ на сайте, который осуществляет электронную торговлю (действует аналогично электронной доске объявлений), товаров, которые имеют особенный порядок обращения, и их получения в форме внутреннего или международного почтового отправления.

4.2. Распространение через сайты, которые специализируются на трансляции видеоизображений эротичного и порнографического характера видеопродукции, изображений порнографического характера, создание и организация функционирования «студий» из изготовлению и распространению такой видеопродукции, обеспечения ее трансляции и изображений в режиме онлайн (с использованием режима «Privat chat»), а также возможно одновременное создание и администрирование соответствующих сайтов. Так, на протяжении четырех лет (с 2009 до 2013 г.) на территории Одесской области действовала организованная группа в составе семи лиц с внутренне и внешне стойкими иерархическими связками, которая из корыстных побуждений, имея целью непосредственное совершение тяжких преступлений, занималась изготовлением с целью сбыта и распространением через Интернет посредством компьютерных программ видеопродукции, изображений порнографического характера [13]. Определив направленность своей преступной деятельности, два лица, действуя как лидеры преступной группы, посредством глобальной сети Интернет познакомились с неустановленными в ходе следствия владельцами таких сайтов как «777LiveCams», «CamContacts», «ImLive», «LiveJasmin», «Streamate», которые специализировались на трансляции видеоизображений эротичного и порнографического характера. Согласно достигнутой договоренности с владельцами «сайтов» была создана и зарегистрирована студия «Debirs», был получен доступ к отмеченным «сайтам», в режиме on line – то есть реального времени, и началась прямая трансляция видеопродукции и изображений порнографического характера. Лица (клиенты), заинтересованные в пересмотре видеоизображений девушек-моделей, «войдя» на указанные сайты, посредством своих электронных платежных карточек должны были оплачивать время общения в приват-чатах с моделями.

4.3. Предоставление возможности посетителям созданного веб-сайта пересматривать или копировать аудиовизуальные произведения, компьютерные программы, фонограммы, права на которые принадлежат другому лицу. Так, житель г. Вижница Черновицкой области в сентябре 2012 года создал веб-сайт «ost.cv.ua», осуществляя его администрирование с использованием собственного персонального компьютера с целью ведения электронной коммерции и распространения аудиовизуальных произведений без права на это [14].

4.4. Создание условий для азартных игр в форме интерактивного

электронного (виртуального) казино. Так, продолжается следствие в деле касательно 12 граждан РФ, которые наняли около 80 работников для организации и проведения азартных игр в сети. По официальным сообщениям Департамента киберполиции, его работники задокументировали деятельность данной группы лиц, которые организовали в Украине проведения азартных игр в виртуальном (электронном) казино на восьми интернет-площадках [15].

5. Способы преступных действий, связанные с функционированием технологий электронной рассылки, IP-телефонии, которые предназначены для отправления/получения электронных сообщений между пользователями компьютерной/телекоммуникационной сети.

Сегодня эти массовые по характеру технологии позволяют как начинать, так и доводить до логического окончания преступления различной квалификации и степени тяжести: от заведомо неправдивого сообщения о подготовке взрыва (ст. 259 КК Украины) до государственной измены (ст. 111 КК Украины). Однако их обычно используют преступники типа «пользователь низкого уровня» или «преступник-пользователь». Непосредственный способ действий преступника заключается в отправлении/получении электронных сообщений. Действия преступника часто являются следующими.

5.1. Преступник посылает государственным или коммерческим учреждениям неправдивую информацию о «заминировании» зданий (непосредственный способ совершения преступления).

5.2. Преступник посылает представителям иностранных разведок сведения военного характера или конфиденциальную информацию (непосредственный способ совершения преступления), чем наносит вред национальной безопасности и интересам Украины в сфере обеспечения порядка, снижает обороноспособность, создает условия для подрывной деятельности.

5.3. Преступник посылает потерпевшему неправдивую информацию в форме массовой рассылки для введения последнего в заблуждение с целью получения от него информации, нужной для последующего осуществления им трансакции (способ подготовки мошенничества).

5.4. Преступник обманным путем получает от жертвы последующего вымогательства сведения (среди прочего фото- и видеофайлы), которые позорят достоинство, честь или деловую репутацию физического лица (способ подготовки вымогательства).

5.5. Преступник незаконно осуществляет ознакомление с чужой электронной корреспонденцией или содержанием телефонных разговоров, другой корреспонденцией.

6. Способы преступных действий, связанные с функционированием технологий электронных платежных систем, предназначенных для осуществления платежных операций через Интернет. Посредством платежной системы осуществляются оплаты разного назначения, поэтому достаточно часто эту технологию используют одновременно с технологией электронной коммерции. Типичный способ действий преступника заключается в создании фиктивных сайтов, через которые от пострадавших за разные услуги или товары принимаются электронные платежи. Так, работники Причерноморского управления Департамента киберполиции совместно со следователями в г. Одессе разоблачили двух местных жителей, которые, создав фиктивный интернет-ресурс «kadastor.in.ua», принимали оплату услуг кадастрового бюро за оформление и получение земельного участка на территории Одесской области. Для реализации своих преступных намерений преступники собственноручно изготовляли фиктивные договора с использованием реквизитов предприятия «Земельное кадастровое бюро» и скрепляли их поддельной мокрой печатью. Сайт отличался от реального оформлением и доменным именем [16]. Также все чаще в Украине имеют место случаи использования электронных платежных систем для финансирования терроризма.

7. Способы преступных действий, связанные с функционированием технологии сохранения и обработки информации. Собственно, эта технология и стала первоосновой существования киберпространства, поэтому ее положили в основу любого действия с его использованием. Впрочем, если рассматривать использование для преступного действия лишь этой технологии, то стоит учитывать, что преступник имеет право доступа к компьютерной информации и совершает часто преступление, предусмотренное ст. 362 или ст. 330 КК Украины. Способ заключается в основном в копировании электронной информации. Так, в период с декабря 2015 года по января 2016 года гр. О., находясь на должности заместителя начальника отдела технического сопровождения управления планирования технического обеспечения вооружения Вооруженных Сил Украины, имея доступ к документам, которые содержат служебную информацию в сфере обороны страны, выполняя задание представителя иностранной организации изготовил электронную копию документа с информацией, которой предоставлено гриф «Для служебного пользования». Отмеченные действия были совершены с целью последующей передачи сведений, что составляют служебную информацию в сфере обороны страны, представителю иностранной организации [17].

8. Способы преступных действий, связанные с функционированием вредоносного программного обеспечения. Это программное обеспечение преступники (по типу «уверенный пользователь», «опытный пользователь» и «профессионал») по собственной инициативе или по заказу третьего лица разрабатывают и/или распространяют для получения несанкционированного доступа к компьютеру с целью несанкционированного доступа к информации и причинения вреда. Так, житель г. Белая Церковь на заказ неустановленного лица осуществлял DDoS-атаки посредством предварительно скопированного из сети программного средства «Bleck Energy», не установленное следствием лицо предоставило ему возможность одновременно с 1000 компьютеров осуществить обращение на тот или иной сервер, IP-адрес или ресурс в сети Интернет, что приводило к блокированию их работы [18]. Такого рода преступления традиционно квалифицируют по соответствующей части ст. 361 КК Украины. Однако это

является типичным лишь при условии невозможности установить в ходе следствия конечную цель действий преступника (подготовка к совершению корыстных преступлений).

Выводы. Предложенные группы способов не являются исчерпывающими, но сегодня они объективно отражают интерактивный характер способов преступной деятельности с использованием обстановки киберпространства. Знание типичных способов совершения преступлений с использованием обстановки киберпространства, закономерных связей между интерактивными элементами механизма преступления позволит следователю в ходе расследования конкретного уголовного правонарушения методически обоснованно отнестись к организации досудебного следствия.

Список использованной литературы:

1. Батурин Ю. М. Проблемы компьютерного права. М.: Юридическая литература, 1991. 272 с.
2. Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: Навч. посібник. К., 1994. 72с.
3. Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. Б. П. Смагоринского. М., 1996. 182 с.
4. Крыгин С.В. Расследование преступлений, совершаемых в сфере компьютерной информации: дис. … канд. юр наук. Н. Новгород, 2002. 200 с.
5. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ: монографія / за редакцією О. О. Подобного. Одесса, 2011. 216 с.
6. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року, № 74/98-ВР. URL: http://zakon5.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80
7. Слепухина А. С. Компьютерные информационные технологии: курс лекций предназначен для студентов факультета экономики и права специальности «Менеджмент». Витебск: УО ФПБ ВФ МИТСО, 2009. 201 с. URL: http://life-prog.ru/1_21247_kurs-lektsiy.html
8. Информатика для гуманитариев: учебник и практикум для академического бакалавраты / Г. Е. Кедрова и др. М., 2018. 439 с.
9. Вирок по справі № 404/3962/16-к від 15 липня 2016 року Кіровського районного суду міста Кіровограда. URL: http://reyestr.court.gov.ua/Review/59029350
10. Вирок по справі № 1-кп/336/67/2013 від 26 лютого 2013 року Шевченківського районного суду м. Запоріжжя. URL: http://reyestr.court.gov.ua/Review/29608881
11. Вирок по справі № 182/3014/15-к від 2 грудня 2015 року Нікопольського міськрайонного суду Дніпропетровської області. URL: http://reyestr.court.gov.ua/Review/54012641
12. Вирок по справі № 569/10782/17 від 27 липня 2017 року Рівненського міського суду Рівненської області. URL: http://reyestr.court.gov.ua/Review/67942562
13. Вирок по справі № 522/6835/14-к/ від 06 червня 2016 року Колегії суддів Приморського районного суду м. Одеси. URL: http://reyestr.court.gov.ua/Review/58207973
14. Вирок по справі № 713/2307/13-к від 12 грудня 2013 року Вижницького районного суду Чернівецької області. URL: http://reyestr.court.gov.ua/Review/36016798
15. Поліція оголосила підозру організаторам кількох онлайн-казино. Офіційний сайт Департаменту кіберполіції. URL: https://cyberpolice.gov.ua/news/policziya-ogolosyla-pidozru-organizatoram-kilkox-onlajn-kazyno-5427/
16. На Одещині кіберполіція виявила фіктивний сайт земельного кадастрового бюро Офіційний сайт Департаменту кіберполіції. URL: https://cyberpolice.gov.ua/news/na-odeshhyni-kiberpolicziya-vyyavyla-fiktyvnyj-sajt-zemelnogo-kadastrovogo-byuro-7030/
17. Вирок по справі № 761/12994/17 від 24 травня 2017рокуШевченківськогорайонногосуду м. Києва URL: http://reyestr.court.gov.ua/Review/66711667
18. Вирок по справі № 1-7/2010 від 05 жовтня 2010 року Білоцерківського міськрайонного суду Київської області. URL: http://reyestr.court.gov.ua/Review/63156830

ИНФОРМАЦИЯ ОБ АВТОРЕ

Самойленко Елена Анатольевна – кандидат юридических наук, доцент, доцент кафедры криминалистики Национального университета «Одесская юридическая академия»

INFORMATION ABOUT THE AUTHOR

Samoylenko Elena Anatolyevna – Candidate of Law Sciences, Associate Professor, Associate Professor of the Department of Criminalistics of National University "Odessa Law Academy"

samoilenko_elena@ukr.net