КРИМИНАЛИСТИЧЕСКИЙ АЛГОРИТМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПРОТИВОДЕЙСТВИЯ КОРЫСТНОЙ ПРЕСТУПНОСТИ

Белоус В. В.

Рассмотрено влияние тенизации рынка нефтепродуктов и хищения бюджетных средств на уровень безопасности отечественных автодорог и защищенности жизни и здоровья граждан. На основе комплексного использования современных информационных технологий предложен криминалистический алгоритм предотвращения корыстной преступности.

Ключевые слова: информационные технологии, криминалистический алгоритм, тенизация рынка нефтепродуктов, фиктивное предприятие, корыстная преступность.

CRIMINALISTIC ALGORITHM FOR THE APPLICATION OF INFORMATION TECHNOLOGIES IN COUNTERACTING LUCRATIVE CRIME

Bilous V. V.

The article deals with the influence of the shadow oil market and embezzlement of public funds on the traffic safety in the country as well as the public security and health. With the comprehensive use of up-to-date information technologies the article suggests a criminalistic algorithm for preventing lucrative crime.

Keywords: information technologies, criminalistic algorithm, shadow oil market, fake enterprise, lucrative crime.

УДК 343.98:343.326

Г. А. Черный, доцент кафедры криминалистики Национальный университет «Юридическая академия Украины имени Ярослава Мудрого», кандидат юридических наук

ЛИЧНОСТЬ КИБЕРПРЕСТУПНИКА В СТРУКТУРЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ТЕРРОРИЗМА

Изучены основные психологические особенности личности киберпреступника, необходимые для организации борьбы с этим видом преступления. Классифицированы и рассмотрены различные психологические типы преступников. Предложена соответствующая им криминалистическая характеристика.

Ключевые слова: терроризм, киберпреступность, личность киберпреступника, информационные преступления.

Терроризм во всех его проявлениях – одно из тяжких и опаснейших преступлений, которое посягает не только на жизнь, здоровье, имущество граждан, но и на фундаментальные устои самого государственного устройства. В ст. 1 Закона Украины «О борьбе с терроризмом» предусмотрен такой

вид терроризма, как технологический терроризм. Технологический терроризм рассматривается как преступления, совершаемые с террористической целью с применением компьютерных систем и коммуникационных сетей, включая их захват, вывод из строя, которые прямо или опосредовано создают или угрожают возникновению угрозы чрезвычайных ситуаций и создают опасность для персонала, населения и окружающей среды, условия для аварий и катастроф техногенного характера.

Необходимость изучения киберпреступлений вызвана чрезвычайно большим количеством преступлений, охватываемых этим понятием, хотя до сих пор его толкуют как в узком смысле – преступления, ответственность за которые предусмотрена разделом уголовного кодекса соответствующей страны (гл. 16 УК Украины устанавливает уголовную ответственность за преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей, сетей электросвязи); гл. 28 УК РФ предусматривает ответственность за преступления в сфере компьютерной информации), так и в широком – любые преступления, совершенные с помощью электронных устройств. Для исследования личности преступника более подходит широкое толкование термина «киберпреступление», что соответствует и рекомендациям экспертов ООН.

Основной особенностью киберпреступлений, связанных с терроризмом, является среда их совершения – образованное электронным устройством и их сетями киберпространство (или виртуальное пространство). В условиях киберпространства существенно меняются психологическое содержание взаимосвязей личность преступника – предмет посягательства, а также личность преступника – личность потерпевшего, которые из непосредственных, прямых превращаются в опосредованные*:* преступник – электронное устройство (Сеть) – потерпевший (предмет преступления), что ведет к устранению материальной составляющей как действий человека, так и социального взаимодействия. При этом «виртуальные» предметы психологически кажутся более доступными, в том числе для незаконного завладения ими.

Подтверждением менее ответственного отношения к нематериальным, чем к материальным предметам является широко распространенное нарушение авторских прав. Согласно предварительным результатам опроса «Культура копирования в США и Германии», проведенного по заказу Американской ассамблеи, около 46 % взрослых жителей США покупали, копировали или загружали с нарушением авторских прав музыку, ТВ-программы или фильмы, а среди людей в возрасте 18–29 лет 70 % пользовались пиратскими аудио- или видеофайлами[1]. Любые же действия в таких условиях воспринимаются изначально как нематериальные по природе, соответственно, не несущие материальных, «серьезных» последствий. Как справедливо отмечает директор Центра безопасного и ответственного использования Интернета Н. Виллард, «информационно-коммуникационные технологии существенно ограничивают обратную связь, любое чувство осязаемой обратной связи наших действий. Поэтому отсутствует влияние осознания того,

[1] См.: Copyright Infringement and Enforcement in the USA: A Research Note [Электронный ресурс]. — Режим доступа : http://piracy.ssrc.org/wp-content/uploads/2011/ll/AA-Research-Note-Infringement-and-Enforcement-November-2011.pdf. — P. 2.

что мы причинили вред, но также мы считаем, что наше поведение не может причинить никакого вреда, потому что мы не видим вреда»[1].

Как показали DoS-атаки (атака типа «отказ в обслуживании», от англ. Denial of Service) на сайты государственных органов Украины, которые произошли после закрытия файлообменного сервиса ex.ua (где находился «пиратский» контент) и к совершению которых были причастны обыкновенные пользователи, «пиратство» имеет прямую взаимосвязь с более серьезными видами киберпреступлений и способствует распространению киберпреступности в целом.

Важным фактором психологического характера, присущим киберпространству, является возможность сохранения полной анонимности пользователя устройства или Сети (за исключением технической информации о подключении к Сети, способы сокрытия которой также существуют). Анонимность позволяет не только не быть идентифицированным в определенный момент времени, но и как следствие предоставлять о себе ложную информацию, вступать в социальное взаимодействие, представляясь другим лицом. Очевидно, что в условиях анонимности любой человек ощущает возможность безнаказанно совершать поступки отрицательного характера, при этом отсутствие эффективных механизмов порицания только усиливает желание совершать негативные действия, особенно, если первопричина таких действий лежит в реальном мире.

В то же время подобное ощущение безнаказанности не только влияет на отдельных лиц, но и создает атмосферу вседозволенности, которая способствует дальнейшему распространению и развитию общественноопасных идей. Так, после терактов в Норвегии было установлено, что А. Брейвик был активным посетителем различных праворадикальных Интернет-ресурсов[2]. Адвокат А. Брейвика заявил, что его подзащитный поддавался влиянию со стороны других Интернет-пользователей ультраправых взглядов, в частности со стороны блогера под именем Fjordman, личность которого была установлена только после терактов[3]. Для преодоления возможных негативных последствий анонимности в некоторых городах Китая было введено требование по обязательному использованию реальных данных при регистрации в сервисах микроблогов[4]. Чуть ранее власти Шанхая ввели обязательное использование реальных данных на сайтах знакомств, обосновывая это тем, что «...интернет-анонимность открывает дверь для киберпреступлений, в частности мошенничества...»[5].

[1] Стенограмма Национальной конференции США по киберэтике [Электронный ресурс]. — Режим доступа : http://connect.marymount.edu/etbics/cyberethics/sessions/gensession3.PDF.

[2] См.: How far right views created Anders Behring Breivik [Электронный ресурс]. — Режим доступа : http://mg.co.za/article/2011-07-31-how-far-right-views-created-anders-behring-breivik.

[3] См.: Lippestad: Nettdebattanter har ansvar for terroren. [Электронный ресурс]. — Режим доступа : http://www.aftenposten.no/incoming/Lippestad-Nettde-battanter-har-ansvar-for-terroren-6714368.html.

[4] См.: China tightens microblog supervision. [Электронный ресурс]. — Режим доступа : http://www.chinadaily.com.cn/china/2011-12/22/content_14310618.htm.

[5] Real name registration for matchmaking websites. [Электронный ресурс]. — Режим доступа : http://www.chinadaily.com.cn/china/2011-10/14/content^3904173.htm.

Именно анонимность делает киберпространство «параллельным» нашей обычной жизни и позволяет создавать новый образ собственной личности или сразу несколько образов, отличающихся от реального и не отягощенных психологической обязанностью следовать реальному образу, как это было бы в случае идентификации пользователя. Особенно ярко это выражено в онлайн-играх, где анонимность сопряжена с вымышленным миром. Поэтому весьма вероятно, что у киберпреступников могут встречаться психические отклонения, которые фиксируют у обыкновенных пользователей Интернета: Интернет-зависимость, тревожные расстройства, диссоциативные расстройства личности.

Благодаря перечисленным факторам в киберпространстве, даже в большей степени, чем в реальном мире, возможно возникновение перегрузки социальными контактами, бывает «утрата способности и возможности сосредотачивать внимание на конкретном человеке», что ведет не столько к озлоблению и агрессии, как в реальном мире, сколько к «обесцениванию» каждого из контактов на фоне «триумфа» собственного «Я», обеспеченного субъективным (если даже несолипсическим) восприятием киберпространства[1]. При этом, как обоснованно считает С. В. Бондаренко, «в среде с интенсивными обменами и информационными потоками существует проблема информационного переполнения, при котором снижается острота восприятия авторами фактов девиантного поведения»[2].

В киберпространстве существуют идеальные условия и для сокрытия преступной деятельности за счет таких факторов, как: 1) «самодостаточность» киберпространства как социальной системы – наличие в нем экономических, культурных и других социальных институтов, которые дают возможность человеку почти полноценно существовать, не отходя от компьютера, предоставляя злоумышленникам возможность «маневрировать», сбывать незаконно приобретенную собственность, что, безусловно, играет не последнюю роль в формировании преступного умысла; 2) идеальная среда для «социального раздвоения как социальной игры, связанной со сменой ролей и декораций»[3], в которой перевоплощение не требует изменения собственного внешнего вида или серьезных психологических затрат, как в случае с обыкновенной преступной деятельностью, что позволяет киберпреступникам успешно играть роль законопослушных граждан.

Значительное место отводится психологическим процессам, протекающим при непосредственном совершении киберпреступления. В отличие от подавляющего большинства обыкновенных преступлений совершение киберпреступления не требует, как правило, каких-либо передвижений или принятия каких-либо активных физических действий. Киберпреступник при реализации своего злого умысла находится дома, в компьютерном клубе,

[1] *Федоренко Д.* Криминологические аспекты урбанизации / Д. Федоренко // Юрид. вісник. — 2000. — № 1. — С. 95–99.

[2] *Бондаренко С. В.* Виртуальные сетевые сообщества девиантного поведения / С. В. Бондаренко [Электронный ресурс]. — Режим доступа : http://cyberpsy.ru/2011/06/bondarenko-s-v-virtualnye-setevye-soobshhestva-deviantnogo-povedeniya/.

[3] См.: *Кравченко А. И.* Общая психология : уч. пособие / А. И. Кравченко. — М. : Проспект, 2011. — С. 399.

месте с бесплатным доступом в Интернет, любом другом выбранном им месте, которое для него является комфортным или, по крайней мере, знакомым и привычным. Поэтому киберпреступники могут не ощущать или ощущать в значительно меньшей степени дискомфорт, страх быть случайно обнаруженным и задержанным. Хотя киберпространство и является многогранным социальным пространством, в то же время оно остается искусственно созданной программно-аппаратной средой, деятельность в которой все-таки ограничена техническими рамками, что делает предсказуемыми последствия действий. Это в свою очередь позволяет злоумышленнику не ощущать неопределенности ситуации, планировать свои действия даже при неблагоприятных для него обстоятельствах, а значит, чувствовать себя более уверенно и спокойно во время совершения преступления.

Как уже отмечалось, киберпреступники не имеют возможности адекватно оценивать нанесенный ими вред, а следовательно, и испытывать в полной мере возможное раскаяние. При этом положительные ощущения от «достижения заранее планируемого результата, связанного с совершением преступления, и удовлетворение результатом, которое закрепляет образ акта преступного поведения и облегчает его проведение в дальнейшем», наступают в случае успеха, что ведет к последующему совершению преступлений. Если после совершения обычного преступления «на преступника, как правило, в большей степени начинает воздействовать фактор неопределенности своего положения, обусловленный, с одной стороны, сознанием виновности и боязнью наказания, а с другой – недостатком информации о тех действиях, которые предпринимаются правоохранительными органами для расследования преступления и изобличения виновного», то в случае совершения киберпреступления действие данного фактора может уменьшаться либо исключаться по двум причинам. Во-первых, при совершении специальных киберпреступлений преступники, уверенные в высоком уровне своих знаний и возможностей, а порой и в своей гениальности, предполагают, что не оставили ни единого следа, который мог бы помочь изобличить их. Во-вторых, в настоящее время, особенно в странах СНГ, органы, ведущие борьбу с киберпреступностью, не всегда обладают достаточным интеллектуальным и кадровым потенциалом, что ведет к недооцениванию их киберпреступниками[1].

Поскольку ключевым моментом для юридической практики является установление мотивов и целей совершения преступления, не меньшее значение имеют и факторы, детерминирующие их формирование. Основой же формирования субъективной стороны преступления в целом и потребностей человека как исходных мотивов в частности является социальная среда обитания, особенно ее содержательная часть. Сложность состоит в том, что мотивация киберпреступников формируется сразу в двух пространствах: реальном и киберпространстве. При этом на формирование мотивации большее влияние может оказывать и то, и другое пространство.

Киберпространство по-иному влияет на мотивацию преступного поведения в силу следующих причин: 1) это пространство является внетеррито-

[1] *Чуфаровский Ю. В.* Психология оперативно-розыскной деятельности / Ю. В. Чуфаровский. — 2-е изд., доп. — М., 2001. — С. 19.

риальным и основано на других консолидирующих факторах; 2) в киберпространстве происходят не только взаимодействие, взаимопроникновение и смешивание национальных культур, но и формирование своей собственной культурной среды – киберкультуры. Именно изучение влияния киберкультуры на мотивацию киберпреступников является важной задачей для криминологов, поскольку уже сейчас группы хактивистов[1], подобные Anonymous или LulzSec, совершают тяжкие преступления, явно исходя из мотивов, сформированных в киберсреде.

В киберпространстве, как в фактически параллельной реальному миру социальной системе, вместе со смешением национальных культур и зарождением собственной происходят те же процессы с социальными нормами. Некоторые из социальных норм в киберпространстве отмирают, ибо являются неприменимыми, но при этом под воздействием ряда негативных факторов, присущих киберпространству, формируются новые нормы. Можно предположить, что поскольку киберпространство играет достаточно большую роль в жизни молодежи, то в сознании молодых активных пользователей Интернета происходит замещение социальных норм нормами киберпространства, точно так же могут нивелироваться социальные нормы реальной жизни, неприменимые во Всемирной сети. Стоит согласиться с британским ученым А. Даффом, который утверждает, что современное информационное пространство ведет к нормативному кризису во всех сферах человеческой деятельности: экономике, политике, культуре и др.[2] Подобное пограничное состояние в свою очередь отрицательно влияет и на структуру личности преступников.

Как показывает сложившаяся ситуация, в борьбе с киберпреступностью и терроризмом вообще необходим мультидисциплинарный подход. Поэтому создание эффективной системы противодействия киберпреступлениям требует активизации исследований психологии киберпреступников и подготовки кадров в этом направлении.

ОСОБИСТІСТЬ КІБЕРЗЛОЧИНЦЯ В СТРУКТУРІ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ТЕРОРИЗМУ

Чорний Г. О.

Вивчено основні психологічні особливості особистості кіберзлочинця, які виявляються при здійсненні злочинів терористичної спрямованості, з урахуванням узагальнення наукових праць вітчизняних і закордонних криміналістів. Особливу увагу приділено чинникам, що впливають на формування злочинного наміру злочинця, до яких належать можливість існування особи в єдиній інформаційній системі (Мережі) і здійснення нею віртуальних комунікаційних функцій, а також роздвоєння особистості на складові через відсутність безпосереднього спілкування з оточенням. У підсумку зроблено висновок про необхідність мультидисциплінарного підходу до вивчення розглянутої проблеми.

[1] Хактивист (англ. hacktivist) – лицо, использующее компьютерные сети для распространения той или иной идеологии.

[2] См.: *Duff A.* The Normative Crisis of the Information Society / *A. Duff* [Электронный ресурс]. — Режим доступа : http://www.cyberpsychology.eu/view.php?cisloclanku=2008051201.

Ключові слова: тероризм, кіберзлочинність, психологія особистості кіберзлочинця, комп'ютерні та інформаційні злочини.

THE CYBERCRIMINAL'S PERSONALITY IN THE STRUCTURE OF CRIMINALISTIC DESCRIPTION OF TERRORISM

Chernyi H. A.

With reference to the generalized experience of both domestic and foreign criminalists the article deals with the main psychological peculiarities of the cybercriminal's personality that can be revealed in terrorism crimes. The article focuses on the factors that develop the criminal's intent of felon which include both the person's capacity to exist in the single information system (the Net) and his/her performance of communication functions, as well as the personality split into elements caused by the lack of real communication with people around; it concludes that the research into this problem requires a multidisciplinary approach.

Keywords: terrorism, cybercrime, the psychology of the cybercriminal's personality, computer and information crimes.

УДК 343.123.52

С. В. Міронов, заступник прокурора Харківської області

СПОСОБИ (ФОРМИ) ПЕРЕВИЩЕННЯ ВЛАДИ АБО СЛУЖБОВИХ ПОВНОВАЖЕНЬ СПІВРОБІТНИКАМИ ПРАВООХОРОННИХ ОРГАНІВ

За результатами узагальнення судово-слідчої практики проаналізовано найбільш поширені способи (форми) перевищення влади або повноважень службовими особами правоохоронних органів. Окремо розглянуто дії, які явно виходять за межі наданих прав або повноважень службовій особі, супроводжувалися насильством, застосуванням зброї чи болісними й такими, що ображають особисту гідність потерпілого, діями.

Ключові слова: співробітники правоохоронних органів, службові повноваження, способи (форми) перевищення влади або службових повноважень.

Спосіб злочину як правова категорія виступає об'єктом дослідження кримінального права, кримінології та криміналістики, де кожна з цих галузей знань вивчає його виходячи з власних теоретичних і прикладних завдань. При цьому слід зазначити, що у вітчизняному кримінальному законодавстві відсутнє визначення способу злочину, немає єдності й серед науковців щодо розуміння цієї категорії. Так, правознавці акцентують на об'єктно-предметних умовах, засобах і знаряддях застосування способу. Зокрема, М. І. Панов переконаний, що спосіб притаманний будь-якій вольовій поведінці людини й тому є іманентним злочину як явищу реальної дійсності. Він має місце завжди, незважаючи на те зазначений він у законі чи ні[1]. У свою чергу пси-

[1] Див.: *Панов Н. И.* Основные проблемы способа совершения преступления в советском уголовном праве : автореф. дис. на соискание уч. степени доктора юрид.