Актуальным в этой связи является и вопрос о том, как экономические преступления и киберпреступления могут и должны соотноситься между собой. Следует отметить, что уже сегодня отдельные исследователи говорят об экономической преступности в киберпространстве (Л.Н. Киданова, М.А. Простосердов), а также о формировании экономической киберпреступности (Ю.А. Грачев, И.А. Вишневенский, Д.В. Борцов). С учетом изложенного необходимо понимать, как следует осуществлять квалификацию преступлений, которые находятся «на стыке» экономических отношений и информационных технологий. Знание того, какие процессы происходят в экономической сфере в современных условиях, также является залогом более системной реализации действий, связанных с осуществлением противодействия киберпреступности.

При этом проблематика, связанная с совершением экономических преступлений в новых условиях, не может быть сведена исключительно к добавлению «цифровых технологий» к «традиционным» преступлениям, поскольку важно правильно квалифицировать совершенные деяния: будет ли совершаться в данном случае несколько преступлений (т. е. усматривается множественность преступлений), или же совершается единичное преступление. В связи с изложенным важно разграничивать экономические преступления, при совершении которых тем или иным образом используются новые технологии, и киберпреступления как таковые.

В целом процессы, происходящие в сфере экономической преступности, могут реализовываться разными способами и в рамках различных процессов. На основании проведенного анализа нами были определены следующие основные варианты:

совершение экономических преступлений с помощью компьютера или иных цифровых устройств;

совершение экономических преступлений посредством совершения киберпреступлений;

совершение экономических преступлений в рамках экономических процессов, имеющих цифровую форму.

В первом случае квалификация таких деяний не отличается от квалификации экономических преступлений, совершаемых без помощи компьютера, поскольку в этих преступлениях не усматривается цифровых экономических процессов или операций. Следует отметить, что сегодня почти все аспекты жизнедеятельности человека связаны с использованием той или иной цифровой техники или устройства. Например, почти всегда, в том числе при совершении экономических преступлений, совершаются звонки с телефонов, отправляются письма с использованием компьютеров, иных устройств.

Во втором случае, по нашему мнению, квалификация должна осуществляться по совокупности с киберпреступлениями. Следует отметить, что характер экономических преступлений не изменяется, поскольку, несмотря на цифровую форму отражения экономических операций, сами экономические процессы не имеют цифрового характера.

В третьем случае экономические преступления совершаются в сфере экономических отношений, имеющих цифровую форму. Здесь следует пояснить, что отдельные виды экономической деятельности сегодня осуществляются исключительно в цифровой среде. Это, например, деятельность криптообменников (операторов обмена криптовалют). Цифровые технологии в такой ситуации являются неотъемлемой частью деятельности соответствующих субъектов. В ситуации, когда кибердействия совершаются исключительно с целью влияния на программное обеспечение, такие деяния следует считать преступлениями против компьютерной безопасности. В случае же, когда программные средства используются исключительно с целью влияния на экономические процессы, то имеет место экономическое преступление в цифровой информационной среде. Если же подвергаются посягательству оба объекта, то деяние должно квалифицироваться по совокупности как преступление против компьютерной безопасности и как экономическое преступление.

Таким образом, понимание и разграничение различных видов преступлений является значимым фактором, как при проведении научных исследований, так и в деятельности специалистов в сфере противодействия киберпреступности.

УДК 342.9

М.В. Губич

ТЕОРЕТИКО-ПРИКЛАДНЫЕ ПРОБЛЕМЫ ПОНЯТИЙНО-КАТЕГОРИАЛЬНОГО РЯДА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нормативное правовое установление понятийно-категориального ряда в сфере информационной безопасности обусловлено преемственностью теоретико-методологической основы Концепции национальной безопасности Республики Беларусь (далее – Концепция нацбезопасности), а также спецификой рассматриваемой сферы. При этом нерешенность ряда доктринальных вопросов, особенно в части построения четкого понятийного аппарата, присуща как сфере национальной безопас-

ности, так и ее составляющей – информационной безопасности, что имеет принципиальное значение для построения эффективной системы ее обеспечения.

Анализ положений Концепции нацбезопасности и принятой в ее развитие Концепции информационной безопасности Республики Беларусь (далее – Концепция инфбезопасности) в части определения понятий «риски», «вызовы» и «угрозы» национальной безопасности позволяет сделать вывод, что «риски», «вызовы» и «угрозы» информационной и национальной безопасности понимаются как определенные состояния опасности.

Так, в соответствии с действующей редакцией Концепции нацбезопасности:

угроза национальной безопасности – потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь;

формами угроз в стадии их зарождения и насыщения являются риски и вызовы национальной безопасности.

Однако, как на теоретическом уровне, так и на уровне нормативно-правового регулирования, не выработаны четкие и понятные для правоприменителя критерии и признаки, описывающие моменты перехода одного состояния опасности в другое. Изложенное не позволяет провести четкие границы между рассматриваемыми состояниями, что влечет существенные проблемы при практической реализации положений указанных концепций, а также, в определенной степени, вносит путаницу в нормативные предписания.

В качестве иллюстрации представляется возможным привести следующие примеры:

в соответствии с п. 33 Концепции инфбезопасности «государство осуществляет реагирование на риски и вызовы в информационной сфере в целях предупреждения их трансформации в угрозы национальной безопасности, развития и масштабирования вредоносного воздействия», что противоречит Концепции нацбезопасности, в соответствии с которой риски и вызовы – это формы угрозы;

в соответствии с п. 34 Концепции инфбезопасности государственное реагирование на риски, вызовы и угрозы состоит в локализации последствий и восстановлении нанесенного ущерба (при этом в соответствии с Концепцией нацбезопасности угроза рассматривается как возможность нанесения ущерба и не предполагает нанесения ущерба), в выявлении реализующихся вызовов (при этом в соответствии с Концепцией нацбезопасности вызов является формой угрозы в стадии ее насыщения, что не предполагает реализацию).

Таким образом, необходимым условием построения эффективной системы обеспечения безопасности являются разработка и внедрение

нового подхода к пониманию основных категорий механизма возникновения и реализации угроз информационной безопасности.

По нашему мнению, риск не должен рассматриваться как форма угрозы, так как по своей сущности риск является понятием, отражающим зависимость причинения ущерба от поведения субъекта в ситуации опасности. Что позволяет определить риск информационной безопасности как характеристику деятельности субъекта (объекта) информационной безопасности по предотвращению ущерба, осуществляемой в условиях возможности выбора варианта действий и неопределенности их последствий.

Помимо теоретической значимости предложенного понимания риска информационной безопасности, полагаем возможным подчеркнуть и практическую сторону его внедрения в правовую сферу, а именно – официальное закрепление возможности использования в сфере обеспечения информационной безопасности современных достижений в области риск-менеджмента – системы оценки риска, управления риском и отношениями, возникшими в процессе этого управления. Тем более разработчики Концепции инфбезопасности определили стратегической целью развитие системы обеспечения кибербезопасности, базирующейся на передовых международных подходах управления рисками и предназначенной для реализации долгосрочных мер по их сокращению до приемлемого уровня.

Относительно категории «вызов» следует отметить, что в научной литературе теоретико-методологическая проработка понятия «вызов» является одной из наименее разработанных проблем. Толковые словари предлагают несколько значений данного слова: предложение, требование явиться; сигнал, звонок, которым вызывают в аппаратах связи; призыв к борьбе, состязанию; поступок, оцениваемый как объявление борьбы, как оскорбление общепринятых норм. Иными словами, смысловое значение слова «вызов» применительно к сфере информационной безопасности заключается в описании опасности, исходящей от субъекта, имеющего умысел на причинение ущерба либо эскалацию опасности.

Следовательно, вызов должен рассматриваться как форма угрозы, исходящей от субъекта взаимоотношений в сфере защищаемого интереса, при этом данный субъект обязательно должен быть наделен волей выбора варианта поведения. Этимология рассматриваемого слова указывает, что вызов безопасности не может исходить от объекта, фактора, явления, не наделенного волей (объекты, факторы, явления природного характера, или ими обусловленные).

Таким образом, полагаем возможным определить вызов информационной безопасности как потенциальную или реально существующую возможность умышленного нанесения ущерба национальным интересам в информационной сфере.

Анализ понятия «угроза безопасности» и его употребления в нормативных правовых актах позволяет согласиться с пониманием данной категории, приведенной в Концепции нацбезопасности, в соответствии с которой угроза – потенциальная или реально существующая возможность нанесения ущерба.

Вместе с тем некоторые положения данного нормативного правового акта не в полной мере соответствуют определению рассматриваемого понятия. Так, к числу основных угроз национальной безопасности причислены: деструктивное информационное воздействие, наносящее ущерб национальным интересам; нарушение функционирования критически важных объектов информатизации. Иными словами, к угрозам отнесены воздействия уже причинившие ущерб, что, по своей сути, не соответствует представленному выше подходу к пониманию угрозы как возможности нанесения ущерба.

Следует отметить, что в гл. 19 «Противодействие киберпреступности» Концепции инфбезопасности не используются рассмотренные в настоящей статье понятия, что, в определенной степени, может объясняться относительной новизной борьбы с данными преступлениями, отсутствием устоявшихся понятий и категорий, что естественно для этой интенсивно развивающейся сферы. Однако, как и для всех сфер человеческой длительности, построение эффективной системы противодействия киберпреступности возможно только при наличии сформированной теоретической и правовой основы функционирования. Соответственно, решение обозначенных и иных теоретико-прикладных проблем понятийно-категориального ряда информационной безопасности положительно отразится на решении задач обеспечения информационной безопасности и противодействии киберпреступности.

УДК 342.9

М.В. Губич, Д.А. Шкурко

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ НАРКОПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

Интернет является практически идеальной площадкой для обеспечения коммуникации поставщиков и потребителей наркотических средств, координации деятельности и отмывания денег, что порождает ряд проблем в сфере противодействия наркопреступности в сети Интернет.

Так, виртуализация наркопреступности проявляется в создании интернет-магазинов по продаже наркотиков, оплате посредством электронных платежных систем, криптовалют, общении при помощи различных интернет-мессенджеров и интернет-приложений, осуществляющих шифрование получаемых и передаваемых данных, и т. д.

В докладе Международного комитета по контролю над наркотиками за 2021 г. неоднократно отмечается, что рост наркопреступности во многом связан с использованием перечисленных нами выше возможностей интернета [1].

Стремительное развитие сети Интернет превратило его использование в преступной деятельности в основной ресурс для распространения наркотиков, позволило перейти на бесконтактные способы сбыта наркотиков, что существенным образом изменило весь преступный наркобизнес, а также деятельность правоохранительных органов по противодействию рассматриваемым преступлениям.

Наиболее проблемным полем в сфере противодействия наркопреступности является деанонимизация лиц, причастных к совершению преступлений, связанных с незаконным оборотом наркотиков в сети Интернет, особенно в его теневом сегменте сети – DarkNet, доступ к которому возможен только посредством использования специализированных браузеров и программного обеспечения, например Tor – одна из самых популярных технологий для доступа в DarkNet, представляющая собой систему прокси-серверов, позволяющих устанавливать анонимное сетевое соединение. Данная сеть рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

Программное обеспечение Tor обеспечивает анонимность пользователя в сети Интернет, защищает его от анализа, скрывает IP-адрес используемого технического устройства, что затрудняет для представителей правоохранительных органов обнаружение следов, оставляемых преступниками в сети Интернет. Названные свойства достигаются за счет многоуровневого шифрования передаваемого трафика для нескольких произвольно выбранных узлов сети Tor и последовательной трансляции через эти узлы к получателю. Именно в сети Tor созданы и действуют онлайн-магазины, в которых предлагаются для продажи различные виды запрещенных веществ.

Активное использование в преступной деятельности интернет-мессенджеров, осуществляющих шифрование получаемых и передаваемых данных (Signal, Telegram, Vipole, Jabber и др.), также существенным образом трансформирует деятельность подразделений правоохранительных органов, осуществляющих борьбу с рассматриваемыми преступлениями. Это связано со следующими особенностями рассматриваемых мессенджеров: электронные ключи для расшифровки сооб-