способов, методов, приемов и средств в области организации и реализации обеспечения безопасности различных вычислительных устройств;

природы возникновения и реализации различных каналов утечки информации;

вопросов в области организации и реализации обеспечения технической защиты информации, а также криптографической и стеганографической защиты информации;

вопросов в области различных инцидентов, возникающих на базе имеющегося у «пользователя» аппаратного обеспечения, программного обеспечения, информационных ресурсов, среды передачи, а также правил и алгоритмов реагирования на них и их детальную обработку и др.

УрЮИ МВД России на базе имеющихся компьютерных классов, полигонов, центров и других объектов также осуществляет проведение киберучений для закрепления у обучающихся компетенций, приобретаемых ими на учебных занятиях и в ходе самостоятельного изучения разделов учебной дисциплины «Основы кибербезопасности» в рамках внеаудиторной самостоятельной работы.

После завершения 2021/2022 учебного года и начала 2022/2023 учебного года в УрЮИ МВД России, помимо достаточно большого количества положительных моментов от появления в учебных планах учебной дисциплины «Основы кибербезопасности», можно выделить ряд потребностей субъектов образовательного процесса в рамках совершенствования методики проведения учебных занятий.

При этом достаточно важным направлением в области организации и реализации образовательного процесса является рассмотрение вопроса о необходимости оснащения автоматизированных рабочих учебных мест обучающихся (с позиции практической реализации):

системами, основанными на реализации сбора и анализа информации о тех или иных событиях, появляющихся на базе имеющихся у «специалиста» аппаратного обеспечения, программного обеспечения, информационных ресурсов и среды передачи (SIEM);

системами, основанными на реализации фильтрации трафика организации, учреждения, предприятия, а также его анализа (DLP).

Полагается, что учебная дисциплина «Основы кибербезопасности» может также найти свое отражение и в образовательных организациях системы МВД государств – участников МПА СНГ для формирования у обучающихся данных организаций компетенций в области организации кибербезопасности и обеспечения противодействия киберпреступности.

УДК 343.79

М.Г. Головенчик

КИБЕРПРЕСТУПНОСТЬ И ЭКОНОМИЧЕСКАЯ ПРЕСТУПНОСТЬ: ПРОБЛЕМЫ СООТНОШЕНИЯ

В соответствии с Концепцией информационной безопасности Республики Беларусь под киберпреступлениями понимаются предусмотренные Уголовным кодексом Республики Беларусь (далее – УК Беларуси) преступления против информационной безопасности. В УК Беларуси данным преступлениям посвящен разд. XII, гл. 31, где рассматриваемые преступления называются преступлениями против компьютерной безопасности. К таким преступлениям, в частности, относится несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации) (ст. 349 УК Беларуси), умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этим системе или сети, повлекшее по неосторожности причинение существенного вреда (ст. 355 УК Беларуси) и др.

Вместе с тем противодействие киберпреступности, в том числе подготовка специалистов в данной сфере, должно учитывать и то, как киберпреступления соотносятся с иными преступлениями, связанными с цифровой информационной средой.

Рассмотрим эту проблематику на примере экономических преступлений, к которым относят преступления, указанные в гл. 25 «Преступления против порядка осуществления экономической деятельности» УК Беларуси. В условиях цифровизации такие преступления также могут совершаться с помощью информационно-коммуникационных технологий, способами, сходными со способами совершения киберпреступлений. В этой связи может быть затруднительно отграничивать их друг от друга в практической деятельности. Так, в частности, ст. 222 УК Беларуси запрещает изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам. Последующее получение доступа к счетам или электронным кошелькам ставит вопрос о том, что в данном случае совершено: экономическое преступление или киберпреступление?

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-