5. Юдина, М.А. Индустрия 4.0: перспективы и вызовы для общества / М.А. Юдина // Гос. упр. Электрон. вестн. – 2017. – № 60. – С. 197–215.

УДК 343.985

С.А. Корнеев, Э.А. Лопатьевская

КИБЕРПРЕСТУПНОСТЬ И НЕКОТОРЫЕ ВОПРОСЫ ПОДГОТОВКИ ЮРИСТОВ

Одной из новых форм транснациональной преступности является киберпреступность. Когда речь заходит о «киберпреступлении» используются разные понятия – «преступление в сфере компьютерной информации», «преступление в сфере высоких технологий» и др. Чаще всего совершаются преступления, связанные с неправомерным использованием персональных данных.

Согласно ст. 1 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано; предоставление персональных данных – действия, направленные на ознакомление с персональными данными определенных лица или круга лиц; распространение персональных данных – действия, направленные на ознакомление с персональными данными неопределенного круга лиц; субъект персональных данных – физическое лицо, в отношении которого осуществляется обработка персональных данных.

Интернет стал средством обмена информацией по всему миру. Размещая в сети Интернет свою персональную информацию, гражданин может создать условия для совершения в отношении себя киберпреступлений.

Уголовная ответственность за киберпреступления предусмотрена в ряде статей Уголовного кодекса Республики Беларусь: ст. 212 «Хищение имущества путем модификации компьютерной информации»; ст. 349 «Несанкционированный доступ к компьютерной информации»; ст. 350 «Уничтожение, блокирование или модификация компьютерной информации»; ст. 352 «Неправомерное завладение компьютерной информацией»; ст. 354 «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств»; ст. 355 «Нарушение правил эксплуатации компьютерной системы или сети».

В соответствии со ст. 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации; информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Активное использование информационных технологий почти во всех сферах жизнедеятельности предполагает повышение требований к подготовке юристов.

По нашему мнению, в системе подготовки юридических кадров, наряду с необходимостью изучения требований по обеспечению надежности защиты информации на основе технических и программных средств, должны рассматриваться и правовые нормы, направленные на сохранность ведомственной информации и противодействие киберпреступности.

Следовательно, учебный анализ правовых норм должен предшествовать изучению методов по защите информации на основе технических средств и систем и противодействию киберпреступности.

Одним из направлений подготовки специалистов – юристов является включение в учебные программы вопросов по противодействию киберпреступлениям, предусматривающих не только теоретическую, но и практическую подготовку. Отдельные вопросы по противодействию киберпреступности можно включать в программу преддипломной практики.

Считаем также целесообразным вопросы по противодействию киберпреступности предусматривать в программах научно-практических конференций, приводимых на юридических факультетах с участием специалистов в данной сфере.

В заключение отметим, что в современных условиях важен системный, комплексный подход при подготовке специалистов, обладающих навыками по обеспечению сохранности ведомственной информации и противодействию киберпреступности.

УДК 393.985

В.В. Кравец

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ

Стремительное развитие информационных технологий, их широкая доступность и мгновенная возможность обмена информацией в сети Интернет, преобразует интернет-пространство в мощное оружие, целью которого является воздействие на сознание людей.

В Концепции национальной безопасности Республики Беларусь выделены основные национальные интересы белорусского государства в информационной сфере, которыми являются: «реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации; формирование и поступательное развитие информационного общества; равноправное участие Республики Беларусь в мировых информационных отношениях; преобразование информационной индустрии в экспортно-ориентированный сектор экономики; эффективное информационное обеспечение государственной политики; обеспечение надежности и устойчивости функционирования критически важных объектов информатизации». При этом для обеспечения реализации указанных выше национальных интересов в данной области в первую очередь правоохранительные органы должны обратить внимание на предупреждение распространения в сети Интернет фальсифицированной, недостоверной и запрещенной информации.

В Законе Республики Беларусь от 17 июля 2008 г. № 427-З «О средствах массовой информации» определен конкретный перечень информации, распространение которой в средствах массовой информации запрещено. Одним из пунктов выделяется запрет распространения «информации, направленной на пропаганду войны, экстремистской деятельности или содержащей призывы к такой деятельности, порнографии, насилия и жестокости, в том числе пропагандирующей или побуждающей к самоубийству, другой информации, распространение которой способно нанести вред национальным интересам Республики Беларусь или запрещено настоящим Законом, иными законодательными актами».

Опыт борьбы с экстремизмом был получен правоохранительными органами в 2020 г., когда экстремистские формирования в различных Telegram-каналах и чатах собирали аудиторию людей, где экстремистская деятельность преподносилась обывателям как законная деятельность. Проблема в первую очередь состояла в том, что простые люди, ввиду удобства использования мессенджера Telegram, очень быстро могли прочесть информацию именно в экстремистских Telegram-каналах, которые, с учетом материальной поддержки из-за рубежа, воздействовали на сознание граждан, и под предлогами «ложного патриотизма», возможности заработать, анонимности и возможности скрыться от правосудия побуждали людей к совершению противоправных деяний. В свою очередь, государственные каналы массовой информации не акцентировали внимание на распространение информации в мессенджере Telegram, а преимущественно использовали традиционные способы распространения информации по телевизионным каналам, размещении на официальном сайте, в газетах и других устоявшихся в нашем обиходе источниках, которые

предоставляют информацию в обусловленное программное время, а преимущество интернет-сообществ и чатов состояло именно в удобстве подачи информации в любое время суток. Экстремистские организации подталкивали людей, проживающих на территории белорусского государства, к активным антиобщественным действиям (забастовки, неповиновение и активное сопротивление сотрудникам милиции, несанкционированные массовые мероприятия и др.).

С помощью разнообразных интернет-ресурсов организованные экстремистские формирования обеспечивают идеологическую подготовку своих пользователей, осуществляют сбор средств и непосредственно подготовку к проведению и совершению преступлений экстремистской направленности. Контент основных интернет-ресурсов, носящий экстремистский характер, отличается продуманной теоретической базой, спектром методов информационно-психологического воздействия на пользователей. Исходя из вышеизложенного, можно сделать вывод: появилась новая форма экстремизма – киберэкстремизм, которая по своей сути никак не отличается от экстремистской деятельности, однако представляет собой новую возможность ее реализации.

Сегодня можно говорить о том, что государственные новостные каналы, а также органы внутренних дел активно используют в своей непосредственной деятельности социальные сети, интернет-сообщества и чаты для проведения активного патриотического воспитания и разоблачения фейковой информации. Осуществляется также оперативное противодействие уже имеющимся экстремистским формированиям, благодаря новой редакции Закона Республики Беларусь «О противодействии экстремизму», вступившей в силу с 16 июня 2021 г., Министерство внутренних дел Республики Беларусь и Комитет государственной безопасности Республики Беларусь имеют право признавать экстремистскими формированиями группы граждан, осуществляющих экстремистскую деятельность, либо оказывающих иное содействие такой деятельности.

Анализ опыта по противодействию киберэкстремизму позволяет сделать вывод о том, что для эффективного противостояния его влиянию необходимы создание и функционирование на постоянной основе популярных, легкодоступных интернет-ресурсов, посредством которых возможен постоянный диалог с людьми, проживающими на территории белорусского государства. На данный момент указанное направление деятельности активно развивается органами внутренних дел, однако стоит открытым вопрос создания заинтересованности и привлечения большего числа пользователей для постоянного ознакомления с предоставляемой информацией.

Таким образом, для непосредственной борьбы с уже функционирующими интернет-ресурсами экстремистского характера необходи-

мо наладить работу по мониторингу интернет-пространства с целью оперативного реагирования на размещаемые материалы, для признания их экстремистскими, разоблачения фейковой информации и, соответственно, привлечению лиц, разместивших данный контент, к установленной законом ответственности. Не следует забывать о необходимости информационно-просветительской работы с населением, в большей степени в среде подрастающего поколения, для популяризации патриотизма, уважения к истории своей страны, веротерпимости и законопослушности.

УДК 343.3

Д.К. Куаныш

ОСОБЕННОСТИ МОШЕННИЧЕСТВА В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Одним из современных явлений, которое коренным образом повлияло на развитие глобальных процессов в мировом сообществе, стало интенсивное совершенствование информационно-коммуникационных технологий. Масштаб культурных, социальных, экономических, политических, правовых изменений, вызванных распространением сетевых компьютерных коммуникаций, позволяет многим ученым считать их отражением начала нового этапа в истории человеческой цивилизации. Использование глобальной компьютерной сети Интернет выступает одной из важнейших предпосылок глобализации межгосударственных отношений и построения информационного общества.

Избрав цель занять достойное место среди ведущих стран мира в области развития информационного общества, Республика Казахстан активно развивает собственную информационную и телекоммуникационную инфраструктуру, формирует адекватную политику по обеспечению информационной безопасности.

Киберпреступление – это преступление, совершенное дистанционно в киберпространстве, направленное на причинение вреда охраняемым законом разнородным общественным отношениям, совершаемое с использованием информационно-телекоммуникационных сетей, средств и устройств с доступом в киберпространство. Киберпреступление обязательно обладает такими признаками, как противоправность, общественная опасность, виновность и наказуемость.

Исследование признаков и особенностей киберпреступлений нередко вызывает определенные сложности. Во-первых, это отсутствие в юридической науке и правоприменительной практике устоявшегося терминологического аппарата для данной группы противоправных деяний.

Общественная опасность рассматриваемых уголовных правонарушений заключается прежде всего в том, что они нарушают права и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в информационной сфере, наносят вред конфиденциальности, целостности, сохранности и доступности информационных ресурсов, информационных систем и инфраструктуры связи [1].

Квалификация, раскрытие и расследование уголовных правонарушений в сфере информатизации и связи остается до сих пор нелегкой задачей для сотрудников правоохранительных и специальных органов Республики Казахстан. К причинам подобного рода можно отнести:

отсутствие обобщений следственной и судебной практики;

соответствующих научно обоснованных методических и криминалистических рекомендаций;

специального учебного курса, при подготовке в учебных заведениях системы МВД сотрудников следственно-криминалистической специализации, а также следователей, дознавателей, оперативных сотрудников на курсах повышения квалификации и переподготовки;

достаточной подготовленности сотрудников правоохранительных органов к работе со специфическим видом доказательственной информации, возникающей в результате совершения этих уголовных правонарушений, и рядом других факторов.

Для понимания и уточнения некоторых особенностей исследуемой нами киберпреступности необходимо остановиться на отдельных составах преступлений, где объектом выступают в первую очередь общественные интересы в сфере информационной безопасности.

Объектом уголовного правонарушения, предусмотренного ст. 205 Уголовного кодекса (УК) Республики Казахстан, являются права и законные интересы граждан и организаций на конфиденциальность информации, информационных систем и сетей телекоммуникаций. Предметом рассматриваемого уголовного правонарушения выступают: информация, охраняемая законом и содержащаяся на электронном носителе; информационная система, в том числе информационная система государственных органов; сеть телекоммуникаций; государственные электронные информационные ресурсы.

Объективная сторона рассматриваемого уголовного правонарушения выражается в неправомерном доступе к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций. Неправомерный доступ к охраняемой