сантов учреждений образования МВД Республики Беларусь, сотрудников подразделений криминальной милиции для проведения различных мероприятий по обучению навыкам информационной безопасности).

В целях выработки наиболее оптимальных путей повышения эффективности борьбы с киберпреступностью в Республике Беларусь посредством более тесного взаимодействия граждан и организаций с правоохранительными органами считаем необходимым продолжить изучение рассматриваемой проблематики в рамках комплексного исследования, в котором будут изучены ее правовые, социальные, психологические и иные аспекты.

УДК 343.9

Д.Д. Урстенова

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

В наше время наступила информационная эра, т. е. переход от традиционной индустрии промышленности к оцифрованной, компьютеризованной индустрии, направленный на моментальный обмен информации, что послужило началом цифровой революции во всех сферах жизни человечества. В своем послании Глава государства Президент Республики Казахстан Касым-Жомарт Токаев пояснил, что «Цифровизация – это не следование модной тенденции, а ключевой инструмент достижения национальной конкурентоспособности. Прежде всего предстоит устранить цифровое неравенство, обеспечить максимальный доступ к интернету и качественной связи для всех граждан. Сегодня это такая же базовая потребность, как дороги и электричество» [1]. В период всеобщей цифровизации правительства и экономических процессов преступность трансформируется под современные реалии.

Мошенничество в сети Интернет на данный момент имеет масштабный характер, о чем свидетельствуют статистические данные регистрации уголовных правонарушений. Преступники используют все более изощренные способы и методы совершения мошенничества в сети Интернет, что даже самые бдительные граждане попадаются на ловушку преступника.

В настоящее время в интернет-ресурсах Казахстана имеется огромное количество онлайн-сервисов объявлений (olx.kz, krisha.kz, kolesa.kz и т. д.), которые содержат различные виды услуг, купли-продажи и т. д.

Каждый пользователь сети Интернет может выставить любое объявление без указания достоверных личных данных и описание товара или услуги. Проверить достоверность данных пользователей не предоставляется возможным, так как затрагивает права человека, указанные в Законе Республики Казахстан от 21 мая 2013 г. № 94-V «О персональных данных и их защите».

Во всем цивилизованном мире права человека стоят на первом месте и защищаются международными соглашениями, такими как Международный пакт о гражданских и политических правах (International Covenant on Civil and Political Rights – ICCPR) и Всеобщая декларация прав человека (Universal Declaration of Human Rights – UNDP). Анонимность – это невозможность идентифицировать субъект. Также это не допускает возможности несанкционированного использования персональной информации, которой могут воспользоваться в корыстных целях.

Однако у данного утверждения имеется обратная сторона, так как то, что нельзя контролировать, может быть опасным. Вопрос о защите персональных данных пользователей сети Интернет с правовой точки зрения был не до конца изучен. Республика Казахстан при форсированном развитии цифровизации и почти полном переходе документооборота в цифровой формат параллельно проводит законотворческую работу по изменению законодательства с целью наиболее качественной защиты персональных данных граждан.

Так, по мнению К.В. Кецко, для субъектов электронной коммерции анонимность в сети Интернет, с одной стороны, является преимуществом, с другой – вызывает опасения участников, несет определенные риски, в частности, доступность внешнего проникновения, спам-атаки, создание сайтов-дубликатов [2].

Другие авторы относят анонимность в сети Интернет к проблемам правового регулирования цифровых технологий, связанным с реализацией прав и свобод граждан. Они утверждают, что анонимность пользователя – это его конституционная гарантия, обеспечивающая охрану тайн его личной жизни. При этом авторы не исключают ограничение анонимности, когда она используется во вред охраняемым законом общественным отношениям [3].

Сегодня на просторах глобальной компьютерной сети Интернет имеются различные фишинговые сайты, с помощью которых интернет-мошенники осуществляют преступные деяния в сети Интернет.

Фактической профилактикой интернет-мошенничества занимаются как правоохранительные органы, так и государственные структуры, кроме того и IT-гиганты, такие как Google, Yandex и др. Кроме того, профилактикой занимаются и субъекты предпринимательской дея-

тельности – банки, крупные корпорации, операторы сотовой связи, организации, занимающиеся разработками IT-продуктов, другие организации и физические лица, так или иначе заинтересованные в информационной безопасности в сети Интернет.

Список использованных источников

1. Послание Главы государства Касым-Жомарта Токаева народу Казахстана [Электронный ресурс] // Президент Республики Казахстан : офиц. сайт. – URL: http://https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-183048 (дата обращения: 01.09.2022).

2. Кецко, К.В. Преступность в сфере электронной коммерции / К.В. Кецко // Рос. следователь. – 2021. – № 9. – С. 58–63.

3. Уваров, А.А. Проблемы использования цифровых технологий при реализации прав и свобод граждан / А.А. Уваров // Право и цифровая экономика. – 2020. – № 2. – С. 5–11.

УДК 343.918.2

И.А. Фомина

ТИПОЛОГИЯ ЛИЧНОСТИ КИБЕРПРЕСТУПНИКА ПО ПАРАМЕТРАМ НАПРАВЛЕННОСТИ

Киберпреступность как правовая, практическая и политическая проблема представляет собой прямую угрозу правам человека, общества и государства. Ее большая опасность в том, что современное развитие мира немыслимо без телекоммуникационных систем. Наш современный мир – цифровой мир, где есть место не только новым возможностям, но и рискам. Рост и прогресс цифровых технологий создали совершенно новую платформу для преступной деятельности. Соответственно, перемещение преступности в киберпространство вполне закономерно – это диктует необходимость перепрофилирования не только правоохранительных органов, но и изменения научных исследований в этом направлении, с учетом особенностей киберпространства. Из-за технологических достижений киберпреступность обычно относится к преступлениям, в которых компьютерная сеть используется в незаконных целях, таких как кража конфиденциальных данных, мошенничество, отмывание денег и детская порнография. С развитием технологий появляются и виды киберпреступлений, которые совершают преступники. При этом киберпреступность принимает различные формы, включая хакерство, распространение вредоносного программного обеспечения, программ-вымогателей, фишинг и др. Многие виды ки-

берпреступности являются продолжением существующей офлайн преступной деятельности, поскольку компьютеры и интернет отделили их от географического местоположения преступника, обеспечивая анонимность и защиту от судебного преследования.

Лица, активно использующие киберпространство в своих преступных целях, обладают специфическими, характерными для них характеристиками целей и мотивов, позволяющими классифицировать (объединить) их по параметрам направленности. Благодаря точной типизации потенциальных киберпреступников, сотрудники правоохранительных органов, занимающиеся предупреждением киберпреступлений, лучше понимают, кто такие киберпреступники, какие методы они используют и какие контрмеры могут быть приняты для защиты и предотвращения будущих киберпреступлений.

Следует иметь в виду, что киберпреступники – это, обычно, отдельные лица или небольшие группы. Однако существуют также крупные и высокоорганизованные группы, которые способны проводить массовые целенаправленные атаки. Они относятся к киберпреступности как к бизнесу, даже формируя глобальные сообщества, которые разделяют стратегии и инструменты. Они могут объединять силы для проведения скоординированных атак и обмена украденными личными данными и информацией на своем подпольном рынке.

Киберпреступники широко представлены в так называемой Dark Web, где они в основном предоставляют свои незаконные услуги или продукты. При этом, так как киберпреступность представлена в двух разновидностях: как преступная деятельность, нацеленная на компьютеры, использующие вирусы и другие типы вредоносных программ, и как преступная деятельность с использованием компьютеров для совершения других преступлений, то в рамках деления киберпреступников по параметрам направленности целесообразно выделять:

киберпреступников, нацеленных на компьютеры (могут например, заражать их вредоносными программами, чтобы повредить устройства или остановить их работу; могут использовать вредоносные программы для удаления или кражи данных; могут помешать пользователям использовать интернет или помешать бизнесу предоставлять программные услуги своим клиентам, т. е. атака по типу «отказ в обслуживании» (DoS));

киберпреступников, которые используют компьютер для совершения других преступлений, когда происходит использование компьютеров или сетей для распространения вредоносных программ, незаконной информации, предметов или незаконных изображений (например, наркопреступление, детская порнография, кибертерроризм и др.);

киберпреступников, которые совмещают в себе два типа: делают и то, и другое одновременно. Они могут сначала заражать компьютеры