– для определения порядка использования технического средства в противодействии преступности и установлении истины по делу необходимо определиться с содержанием информации, которую получает субъект борьбы с преступностью. Исходя из этого и формируется алгоритм (последовательность) действий субъекта для получения криминалистически значимой информации с использованием различных технических средств;

– в современных реалиях повсеместное использование криминалистических технологий при выявлении, раскрытии, расследовании и профилактике преступлений должно стать главной целью органа уголовного преследования;

– суды при рассмотрении уголовных дел должны также свободно владеть практикой использования криминалистических технологий в целях установления истины по делу, что позволит при выявлении недостатков в работе органа уголовного преследования правильно использовать имеющийся потенциал технического прогресса;

– особую актуальность приобретает разработка конкретных методических рекомендаций по использованию криминалистических технологий противодействия преступности, связанных с получением доказательственной информации из баз данных различных технических средств некриминалистического назначения.

ЦИФРОВОЕ ПРОСТРАНСТВО КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ

Набатова А. Э.

ГУО «Гомельский государственный университет им. Ф. Скорины»,
ул. Советская, 102, 246003, г. Гомель, Беларусь, jurfac@gsu.by

Рассматривается цифровое пространство как объект криминалистического исследования. Автором дано его понятие, исследована структура и элементы.

Ключевые слова: цифровое пространство; цифровизация; преступность; структура и элементы цифрового пространства.

Современный период развития общества характеризуется формированием новых политических, экономических, социальных, правовых отношений. Для данных процессов существует множество факторов. Ключевым из них, является глобальная цифровизация существенно изменившая формы и механизмы взаимодействия между государственными, предпринимательскими структурами и обществом. В республике более 85% населения являются абонентами глобальной компьютерной сети Интернет, а значит, используют информационные технологии для взаимодействия друг с другом, государственными структурами, банковскими учреждениями, торговыми интернет-площадками по всему миру. Все больше граждан предпочитают знакомиться, общаться, объединяться в сообщества, совершать покупки в Интернете, и в перспективе, данные тенденции будут только усиливаться, переводя в цифровой формат различные взаимодействия.

Указанные обстоятельства неизбежно трансформируют преступность как социально-правовое, исторически изменчивое явление. В связи с чем, мы вступили в этап, когда преступления выходят за границы одной страны, так как совершаются в цифровом пространстве. В подтверждение заявленным тезисам приведем некоторые статистические сведения.

Так, анализ структуры преступности в Республике Беларусь показал следующие тенденции. Достаточно высока доля преступлений в цифровой сфере (ст.ст. 209, 212, глава 31 УК) хотя и наблюдается существенное снижение количественных показателей. Так, в 2020 году было совершено 25 571 киберпреступлений, в 2021 – 15 503, с января по октябрь 2022 года – 11 707 [1; 2]. Например, в 2021 году в Минске было возбуждено 5 196 уголовных дел о киберпреступлениях. Большинство их них совершается путем использования социальной инженерии: «вишинг» и «фишинг» (более 91% от общего количества возбужденных уголовных дел) [3]. За совершение деяний в данном сегменте, а именно за хищения путем использования компьютерной техники и преступления против компьютерной безопасности в 2020 г. было осуждено 1539 чел., в 2021 г. – 1206 [4, с. 152].

Наблюдаются тенденции по цифровой трансформации таких преступлений как разжигание расовой, национальной, религиозной либо иной социальной вражды или розни, реабилитация нацизма, экстремизм, незаконные действия в отношении наркотических средств, психотропных веществ, их прекурсоров и аналогов, изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с участием несовершеннолетних и т.д. Глобальная компьютерная сеть Интернет зачастую выступает местом, средством или орудием совершения указанных деяний.

Некоторые из них имеют существенные количественные показатели в структуре преступности. Например, за преступления, связанные с незаконными действиями в отношении наркотических средств, психотропных веществ, их прекурсоров и аналогов в 2020 г. было осуждено 2002 чел., в 2021 г. – 2050 [4, с. 153]. Еще одной тенденцией последних лет является экстремизм. В республике зарегистрировано свыше 6 тыс. экстремистских преступлений, большая часть которых совершена в 2020-2021 годах. 77% данных преступлений раскрыто, с 2020 г. судами рассмотрено почти 3000 уголовных дел экстремистской направленности в отношении 3 645 лиц. В частности, к лишению свободы осуждено 42% преступников, еще 20% – к ограничению свободы [5].

Таким образом, можно правомерно говорить о цифровой трансформации преступности. Объединяющим фактором данного процесса выступает цифровое пространство, в котором традиционные криминалистические категории такие как следы преступления, время, место, способ, орудия их совершения, личность преступника приобретают цифровое содержание. Цифровое пространство можно рассматривать как самостоятельный объект криминалистического исследования, что представляется весьма актуальным на современном этапе и требует самостоятельного научного осмысления.

Таким образом, объектом исследования в статье выступают закономерности структуры и содержания цифрового пространства как объекта криминалистического исследования. Целью работы является определение цифрового простран-

ства в качестве самостоятельного объекта исследования при раскрытии и расследовании преступлений. Для достижения поставленной цели необходимо решить следующие задачи: дать понятие цифрового пространства; определить его структуру; охарактеризовать его элементы. В качестве методов применим анализ, синтез, системный подход и др.

В республике принято обширное законодательство по вопросам информатизации, цифровизации (Концепции информационной безопасности Республики Беларусь, Государственная программа ««Цифровое развитие Беларуси» на 2021–2025 годы, Закон Республики Беларусь «Об информации, информатизации и защите информации», Указ Президента Республики Беларусь «О кибербезопасности» и др.), в котором содержаться термины и определения, общепринятые для правоприменительной практики в области информатизации, цифровизации. Однако, анализ последних показал отсутствие понятия «цифровое пространство», в связи с чем, возникает необходимость его определения в рамках настоящего исследования.

Все чаще в официальных выступлениях политиков, экономистов, военных, представителей правоохранительных органов используются термины «цифровизация», «цифровое пространство», «цифровая среда». Обусловлено такое использование в силу следующих обстоятельств. Во-первых, произошел переход от информационного к цифровому обществу. Можно говорить о том, что цифровизация – это следующий этап информатизации, когда информация преобразуется в цифровую форму, этап автоматизации и информатизации экономической деятельности и государственного управления, процесс перехода на цифровые технологии, в основе которого лежит не только использование для решения задач производства или управления информационно-коммуникационных технологий (далее – ИКТ), но также накопление и анализ с их помощью больших данных в целях прогнозирования ситуации, оптимизации процессов и затрат, привлечения новых контрагентов и т.д. Во-вторых, существенное расширение возможностей глобальной компьютерной сети Интернет, появление новых сред и технологий в виртуальном пространстве. В-четвертых, нарастание цифровых навыков и компетенций у населения в области применения персональных компьютеров, Интернета и других видов ИКТ, а также непрерывное приобретение соответствующих знаний и опыта в данной сфере в различных возрастных группах.

Отсюда, цифровое пространство можно определить как пространство, интегрирующее цифровые процессы, средства цифрового взаимодействия, информационные ресурсы, а также совокупность цифровых инфраструктур, на основе норм регулирования, механизмов организации, управления и использования [6, с. 258].

Цифровое пространство как системное образование имеет свою инфраструктуру, структуру и ультраструктуру. Цифровая инфраструктура – комплекс технологий и построенных на их основе цифровых продуктов, обеспечивающих вычислительные, телекоммуникационные и сетевые мощности и работающих на цифровой основе. Она включает в себя: ИКТ и интернет-линии (оптоволоконные кабели и др.); вычислительные комплексы различной мощности – от суперкомпьютеров до смартфонов и планшетных компьютеров; вычислительные управляющие встроенные блоки в различные объекты физического мира, начиная от

производственных линий и заканчивая предметами одежды, соединенными в цифровое пространство в единые цифровые системы.

Структура цифрового пространства состоит из: сетевых программных протоколов, обеспечивающих передачу информации по различным сетям, [Интернет, корпоративные сети, одноранговые сети (например, Tor)]; программ и программных платформ, осуществляющих хранение, обработку и предоставление информации – от баз данных до привычных всем операционных систем Windows, Linux; программ-интерфейсов, обеспечивающих восприятие информации конечными пользователями (интерфейсы сайтов, блогов, порталов, приложений и др.);

Ультраструктура цифрового пространства представляет собой информационную среду, где содержатся воспринимаемые пользователем прямые и скрытые смыслы, выраженные в текстах, таблицах, видео– и аудиоконтенте.

Ультраструктура включает в себя общедоступные сетевые ресурсы (сайты, блоги, порталы, социальные сети и др.); защищенные сетевые ресурсы, доступные только для определенных категорий пользователей (информационные ресурсы государственной и корпоративной принадлежности); общедоступные сетевые ресурсы с платным контентом [7, с. 13-33].

Таким образом, из вышеизложенного вытекает, что системообразующим фактором для цифрового пространства выступает Интернет, как среда где происходят большинство цифровых процессов, а также подготавливаются и совершаются преступления. Как и цифровое пространство он имеет свою структуру, которая является объектом криминалистического изучения при раскрытии и расследовании преступлений.

В структуре Интернета можно выделить следующие элементы.

Web 1.0. Наиболее давний сегмент сети, включающий в себя правительственные, корпоративные, общественные, персональные порталы, сайты, блоги, онлайн-средства массовой информации. Все они легко доступны при помощи поисковых систем (например, Yandex, Google и др.).

Web 2.0. Интернет социальных сетей и платформ («ВКонтакте», «Одноклассники», «Facebook», «Инстаграмм» и др.). Контент в этом сегменте Интернета создается в основном самими пользователями, поэтому он получил название социального веба. Из-за политики собственников платформ и социальных сетей, а также из-за требований конфиденциальности они лишь частично видимы для поисковых систем. В этом сегменте ускоренными темпами растет доля видео– и фотоконтента.

Web 3.0. Интернет мобильных приложений, интерфейсы которых размещены на планшетных компьютерах, мобильных телефонах. Он позволяет взаимодействовать с различными приложениями без обращения к поисковым системам, путем установления связи между устройством пользователя и Интернетом.

«Интернет вещей» (IoT). Представляет собой соединенные через Интернет с управляющими центрами встроенные информационные блоки различных объектов физического мира, в том числе производственной, социальной, коммунальной инфраструктуры. Например, к нему относятся технологические линии, системы управления водо– и теплоснабжением и др. В данном сегменте возрастает

доля подключений к Интернету домашнего оборудования, бытовой техники, вплоть до холодильников, стиральных машин и т.д.

«Бодинет». Его основой является микроэлектроника, дающая возможность встраивать элементы, передающие информацию о различных объектах в медицинских, поисковых целях и т.д.

Все выше перечисленное можно определить как «видимый» Интернет. Выделяют также «глубинный» Интернет. В нем находятся сайты, которые не видят поисковые системы, и чтобы попасть на такой ресурс, необходимо знать его точный адрес. Кроме того, вход на страницы в глубинной сети, как правило, возможен через регистрацию пользователя или использование пороля (например, государственные базы данных, библиотеки).

Особое значение для криминалистического изучения имеет «темный» Интернет или Даркнет. Его ресурсы не обнаруживаются поисковыми машинами, а доступ на порталы и сайты возможен только платно или по специальному разрешению на использование ресурсов. По оценкам специалистов в Даркнете около 90% всего ценного научно-технического, технологического, финансово-экономического и другого контента. Объемы данной сети нарастают. Основными причинами такого роста являются, с одной стороны, стремление к архивации всех доступных данных корпоративными пользователями, с другой – желание обладателей ресурсов вывести их из общедоступного пользования в платный сегмент и монетизировать.

Основными сегментами Даркнета являются сеть Tor и платежная сеть криптовалют. Названием этот сегмент сети обязан широкому использованию его ресурсов преступниками, организованными группами для противоправной деятельности, связанной с незаконным оборотом оружием, наркотиками, торговлей людьми, распространением порнографии, незаконными действиями по подрыву государственного суверенитета, кибертерроризмом, экстремизмом.

Как показывает правоприменительная практика, сферой деятельности преступности является все цифровое пространство, и в частности, интернет-пространство. Какие-то сегменты сети используются для сбора информации об объекте и предмете посягательства, подготовки преступления (например, web 1.0, web 2.0), какие-то выступают орудием, средством, местом совершения преступных действий (web 3.0, Даркнет).

Из выше изложенного можно констатировать следующее. На современном этапе есть настоятельная необходимость в научном осмыслении цифрового пространства с позиций криминалистической науки. Возникли предпосылки для формирования самостоятельного научного направления по определению содержания, структуры, элементов цифрового пространства как среды для преступной деятельности. Подобное исследование позволит усовершенствовать как общую теорию криминалистики, так и переформатировать некоторые положения криминалистической техники, тактики и методики.

Библиографический список

1. Число киберпреступлений снизилось почти вдвое. Заместитель председателя СК о тенденциях в области IT-преступлений // БЕЛТА [Электронный ресурс]. – Режим доступа: https://www.belta.by/society/view/chislo-kiberprestuplenij-snizilos-pochti-vdvoe-zampred-sk-o-tendentsijah-v-oblasti-it-prestuplenij-496880-2022/. – Дата доступа: 18.03.2023.

2. Основные направления информационно-пропагандистских групп (декабрь, 2022 г.) // Минский городской исполнительный комитет [Электронный ресурс]. – Режим доступа: https://minsk.gov.by/ru/actual/view/209/2022/inf_ material_2022_12.shtml. – Дата доступа: 18.03.2023.

3. Об отдельных вопросах противодействия преступлениям, совершаемым с использованием возможностей глобальной сети // Министерство связи и информатизации Республики Беларусь [Электронный ресурс]. – Режим доступа: https://mpt.gov.by/ru/ob-otdelnyh-voprosah-protivodeystviya-prestupleniyam-sovershaemym-s-ispolzovaniem-vozmozhnostey. – Дата доступа: 18.03.2023.

4. Статистический ежегодник Республики Беларусь // Национальный статистический комитет Республики Беларусь. – Минск, 2022. – 374 с.

5. Швед: количество экстремистских преступлений в прошлом году значительно уменьшилось // БЕЛТА [Электронный ресурс]. – Режим доступа. – https://www.belta.by/society/view/shved-kolichestvo-ekstremistskih-prestuplenij-v-proshlom-godu-znachitelno-umenshilos-551705-2023/. – Дата доступа: 24.02.2023.

6. Цифровая трансформация. Основные понятия и терминология: сб. статей / редкол. : А. В. Тузиков (пред.) [и др.] ; Нац. акад. наук Беларуси, Объед. ин-т проблем информатики. – Минск : Бел. навука, 2020. – 267 с.

7. Овчинский, В. С. Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. – М. : Норма : ИНФРА-М, 2018. – 352 с.

ПРОБЛЕМНЫЕ ВОПРОСЫ ОРГАНИЗАЦИИ ПОСТАНОВКИ ГРАЖДАН НА УЧЕТ ФОТОГРАФИЧЕСКИХ ИЗОБРАЖЕНИЙ ЛИЦ

Нестер И. С., Жаркевич И. Л.

УО «Академия Министерства внутренних дел Республики Беларусь», пр. Машерова, 6, 220005, г. Минск, Беларусь, info@amia.by

Проводится содержательный анализ процесса постановки отельных категорий граждан на учет фотографических изображений лиц. Излагаются основные проблемные аспекты при взаимодействии органов внутренних дел и Государственного комитета судебных экспертиз Республики Беларусь. На основе анализа практики исследуется деятельность сотрудников экспертно-криминалистических подразделений при использовании автоматизированной системы портретной идентификации. Формулируются рекомендации по совершенствованию процесса межведомственного взаимодействия на примере ведения конкретного криминалистического учета.

Ключевые слова: криминалистические учеты; специальные программы; изображения лиц; взаимодействие; экспертно-криминалистические подразделения