УДК 343.1

О. Н. Родина
курсант 4 курса
факультета подготовки дознавателей
Белгородского юридического института МВД России
имени И. Д. Путилина

Научный руководитель: ***Е. А. Новикова****,*
профессор кафедры уголовного процесса
Белгородского юридического института МВД России
имени И. Д. Путилина,
кандидат юридических наук, доцент

ВИДЕОТЕХНОЛОГИИ КАК ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ СОВЕРШЕНСТВОВАНИЯ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Современное законодательство активно развивается и совершенствуется в течение нескольких лет. Обстановка в обществе накладывает свой отпечаток на законодательную базу любого государства. Цифровые технологии являются следствием нового направления развития в области цифровизации. На законодательном уровне все чаще стали закрепляться информационные научные термины [1].

В глобальном плане цифровизация — это деятельность, при которой технологии внедряются в различные сферы жизни и производства с помощью разных видов цифровой продукции. И эта концепция широко внедряется во всех без исключения странах. Видеотехнологии как принципиально новый правовой феномен в той или иной мере довольно часто используются в нормативно-правовых актах Российской Федерации.

В уголовном процессе понятие «видеотехнологии» активно стало использоваться законодателем со второй половины прошлого столетия. Современный Уголовно-процессуальный кодекс Российской Федерации (далее — УПК) закрепил актуальные аспекты применения видеотехнологий в уголовном судопроизводстве в целях эффективного осуществления судебного процесса.

Ускорение темпов развития современных технологий в обществе позволяет нам сделать вывод о том, что данная область изучения требует постоянного изменения и дополнения в законодательстве Российской Федерации, что делает данную тему актуальной и основной в сфере уголовно-процессуального производства, так как технологии цифровизации успешно внедряются в России на протяжении последних лет.

Процесс цифровизации обладает определенными характеристиками, которые как позитивно влияют на человека, так и негативно. Программное

обеспечение находится в открытом доступе, что может значительно повлиять на повышение цифровой грамотности пользователей. Кроме того, использование цифровых технологий значительно упрощает и ускоряет рабочий процесс. Однако у процесса интеграции продвинутых информационных технологий в условиях активного использования интернет-ресурсов существует множество специфических разновидностей преступной деятельности. Таким образом, появляются новые термины, характеризующие данные явления, например, «киберпреступность» и «кибертерроризм» [2].

Классификация киберпреступности как особого вида преступления теперь позволяет нам идентифицировать лишь конкретные виды и методы киберпреступности. Однако объективно оценить масштабы киберпреступности невозможно, так как законов об интернет-преступлениях недостаточно для удовлетворения современных потребностей правоохранительных органов. Поскольку онлайн-системы не статичны и постоянно меняются и эволюционируют, трудно создать правовую базу для всех видов киберпреступности и основу для выявления преступлений правоохранительными органами.

Хотелось бы отметить, что в системе правоохранительных органов ключевую роль по борьбе с киберугрозами занимают органы внутренних дел, которые, в свою очередь, также уполномочены обеспечивать национальную безопасность Российской Федерации.

Кибербезопасность — это структурный элемент национальной безопасности государства, которому необходимо уделять особое внимание в процессе организации деятельности по наиболее эффективному и оперативному выявлению, предупреждению, пресечению и раскрытию киберпреступлений.

В сентябре 2022 г. начало работу Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий [3]. Таким образом, полномочия по борьбе с данным видом преступлений, а также с компьютерными атаками осуществляются данным Управлением. Взаимодействие с иными министерствами, а именно с Министерством цифрового развития, связи массовых коммуникаций Российской Федерации позволит Управлению оперативно решать служебные задачи [4].

Стоит сказать, что существует множество современных методик выявления и раскрытия преступлений, совершенных с использованием цифровых технологий. Однако можно выделить и появление некоторых недостатков, связанных с тем, что развитие информационных технологий предопределило возникновение новых видов преступлений [5], а также совершенствование преступниками способов сокрытия следов своих деяний.

Современные технологии, используемые в криминалистике, способны выявлять следы преступных действий в сфере компьютерной информации, что также влияет на раскрытие IT-преступлений.

Использование городских видеокамер и нейросетей позволяет осуществлять поиск подозреваемых в совершении преступления, отслеживать маршруты их передвижений, а также потенциальных сообщников, распознавать людей, часто посещающих места совершения преступлений [6].

Объединение усилий деятельности правоохранительных органов и мнений ученых-криминалистов в области расследования и раскрытия преступлений, рассмотрения уголовных дел в суде, криминалистической защиты уголовного судопроизводства позволяет нам изучить целевые требования к производительности и показателям цифровых систем и технологий для целей уголовного судопроизводства, а также криминалистического обеспечения расследования и раскрытия преступлений; правовую оценку возможности использования этих систем и технологий и результатов их обработки в качестве доказательств в уголовном судопроизводстве [6].

Использование видеофиксации при собирании доказательств является немаловажным аспектом в деятельности правоохранительных органов. В начале уголовного преследования и после возбуждения уголовного дела видеозаписи с камер могут являться носителями криминалистически значимой информации. Видеоизображения, полученные с помощью видеокамер систем слежения, могут быть использованы при расследовании преступлений, если они зафиксировали событие преступления, момент появления преступников, их преступные действия, а также его внешний облик.

Видео- и аудиозаписи, полученные с помощью систем слежения, представляют собой новый вид информации, которую сегодня правоохранительные органы могут использовать в борьбе с преступностью не только в качестве ориентира для поиска преступника, но и в качестве доказательства. К системам наблюдения, контроля и обучения в процессе осуществления фиксации относятся системы визуального контроля, системы наблюдения за объектами, расположенными в труднодоступных местах, учебные видео- и телевизионные системы и так далее.

В последнее время системы видеонаблюдения получили очень широкое распространение в практике охраны различных хозяйственных, бытовых объектов, а также личного имущества граждан. Системы видеонаблюдения устанавливаются в аэропортах, на станциях метро, железнодорожных вокзалах, автозаправочных станциях, автомагистралях, в торговых центрах, банках, казино, подъездах жилых зданий. Возможность использования в доказывании фиксации придомовых территорий, а также средств фиксации, размещенных при торговых центрах, значительно ускоряют процесс сбора доказательств и имеют значение при расследовании уголовного дела.

Типы систем видеотехнологий могут также включать в себя роботизированные системы видеонаблюдения со специализированными видеокамерами,

которые используются при работе на месте взрыва или на месте происшествия, связанного с обнаружением взрывных устройств.

Робот используется для контроля труднодоступных зон и деталей объектов (в узких помещениях, в проходах между вагонами, под днищем автомобилей), где установлены камеры видео- и звукозаписи. Камера установлена на вращающейся платформе и с помощью телескопического манипулятора может подниматься на высоту до 2 метров.

Одной из новейших областей применения видеотехнологий является изучение непрозрачных объектов, защищенных от видимых лучей, например, поиск тайника при досмотре, досмотр багажа в аэропортах, дистанционное обнаружение оружия под одеждой, где терагерцовые волны безопасны для организма [7]. В то же время изображения, полученные в терагерцовых лучах, характеризуются высокой контрастностью, хотя компоненты прозрачных объектов имеют высокую плотность. Использование данной системы видеотехнологий в правоохранительных органах позволило бы наиболее эффективно выполнять служебные задачи по поиску орудия совершения преступления и других предметов, имеющих значение по уголовному делу.

Сегодня аудиозапись, в отличие от фотографии и видеосъемки, используется в криминалистической деятельности следователя не только как средство визуально-аудиальной записи хода отдельных следственных действий (например, допроса, очной ставки, проверки показаний на месте и т. д.), но и как техническое средство облегчения работы при предоставлении первоначальной оперативной информации о преступлении, при подготовке отдельных процессуальных документов (например, как средство сбора ориентировочной информации перед началом нескольких следственных действий, а также как средство замены рукописных схем, при осмотре места происшествия, допросе с целью подготовки последующих протоколов).

Таким образом, можно говорить о том, что видеотехнологии являются перспективным направлением совершенствования организации современного уголовного судопроизводства, носят обеспечительный характер и оказывают большое влияние на ход и результаты расследования, что служит доказательственной базой по уголовным делам. Современные тенденции развития законодательства в сфере обеспечения кибербезопасности Российской Федерации позволяют сделать вывод о том, что в настоящий момент организация деятельности органов внутренних дел находится на должном уровне. В связи с созданием Управления видится дальнейшая гармонизация законодательных актов по устранению киберугроз.

Широкое применение достижений науки и техники позволяет правоохранительным органам эффективно использовать системы видеотехнологий в процессе осуществления служебной деятельности, а видео- и звукозапись влияют

на ход проведения оперативно-розыскных мероприятий и следственного действия.

1. Что такое цифровизация и какие сферы жизни она заденет [Электронный ресурс] // Центр 2М : [сайт]. URL: https://center2m.ru/digitalization-technologies (дата обращения: 01.10.2023). Перейти к источнику Вернуться к статье

2. Алиханян К. Р. Организация работы МВД России в системе противодействия киберпреступлениям [Электронный ресурс] // Молодой ученый. 2023. № 2 (449). С. 240–242. URL: https://moluch.ru/archive/449/98865/ (дата обращения: 10.02.2024). Перейти к источнику Вернуться к статье

3. Бегеза В. В. Организация деятельности органов внутренних дел в условиях появления новых вызовов кибербезопасности России // NB: Административное право и практика администрирования. 2023. С. 48–56. Вернуться к статье

4. Основные угрозы информационной безопасности органов внутренних дел [Электронный ресурс] // СёрчИнформ : [сайт]. URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-vooruzhennykh-sil-rf/osnovnye-ugrozy-informatsionnoj-bezopasnosti-organov/?ysclid=lsudlfzbbi398233031 (дата обращения: 05.03.2024). Перейти к источнику Вернуться к статье

5. Самоделкин А. С., Тимофеев С. В. Современные методы выявления и раскрытия преступлений, совершаемых с использованием цифровых технологий // Вестн. Восточ.-Сибир. ин-та МВД России. 2022. № 2 (101). С. 206–215. Вернуться к статье

6. Можно или нужно внедрение цифровых технологий в расследование и раскрытие преступлений? [Электронный ресурс] // Издательская группа «Закон» : [сайт]. URL: https://zakon.ru/blog/2023/07/27/mozhno_ili_nuzhno_vnedrenie_cifrovyh_tehnologij_v_rassledovanie_i_raskrytie_prestuplenij?ysclid=lpe6pzgx7r17370109 (дата обращения: 01.11.2023). Перейти к источнику Вернуться к статье

7. Земляченко В. В. Технические особенности применения современных систем видеонаблюдения сотрудниками органов внутренних дел // Проблемы правоохранительной деятельности. 2020. № 3. С. 61–67. Вернуться к статье