

Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего
образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра
Уголовного процесса

ДИПЛОМНАЯ РАБОТА

на тему: «Производство следственных действий в случаях нетерпящих
отлагательства по уголовным делам о преступлениях, совершенных в сфере
цифровых технологий вопросы теории и практики»

Выполнил: Чинин Даниил Павлович

(фамилия, имя, отчество)

40.05.01 Правовое обеспечение национальной

(специальность, год набора, № группы)

безопасности, набор 2019 г., 191 уч. группа

Руководитель: преподаватель кафедры уголовного
процесса КЮИ МВД РФ, майор полиции

(ученая степень, ученое звание, должность)

Кузнецов Дмитрий Владимирович

(фамилия, имя, отчество)

Рецензент: Заместитель начальника следственной
части ГСУ МВД по Республике Татарстан,
подполковник юстиции

(должность, специальное звание)

Шарафутдинов Булат Фаритович

(фамилия, имя, отчество)

Дата защиты: «__» _____ 2024 г. Оценка _____

Казань 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ	7
§ 1. Понятие и виды преступлений, совершенных в сфере цифровых технологий	7
§ 2. Характеристика составов преступлений, совершенных в сфере цифровых технологий	12
ГЛАВА 2. ОБЩИЕ ПОЛОЖЕНИЯ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА О ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В СЛУЧАЯХ, НЕ ТЕРПЯЩИХ ОТЛАГАТЕЛЬСТВА.....	24
§ 1. Характеристика категории «случаи, не терпящие отлагательства» в уголовно-процессуальном законодательстве России.....	24
§ 2. Характеристика положений уголовно-процессуального законодательства, регламентирующих вопросы производства следственных действий случаях, не терпящих отлагательства.....	29
ГЛАВА 3. ОСОБЕННОСТИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В СЛУЧАЯХ НЕТЕРПЯЩИХ ОТЛАГАТЕЛЬСТВА ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ.....	40
§ 1. Характеристика процедуры расследования уголовных дел о преступлениях, совершенных в сфере цифровых технологий.....	40
§ 2. Производство отдельных следственных действий в случаях, не терпящих отлагательства. Обзор правоприменительной практики	49
ЗАКЛЮЧЕНИЕ	56
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ	62

ВВЕДЕНИЕ

Актуальность темы работы. Процесс информатизации общества, внедрение высоких технологий практически в каждую сферу общественной жизни стало благоприятным условием для возникновения новых способов совершения преступных деяний, когда достижения современной (информационной) науки и техники используются для реализации преступных целей. На данный момент можно наблюдать постепенное изменение характера преступности, что выражается в увеличении количества преступников, специализирующихся на преступлениях, совершаемых с использованием цифровых технологий. Это, в первую очередь, преступления имущественного характера, в частности, дистанционное мошенничество, преступления, связанные с незаконным оборотом запрещенных предметов (оружие, боеприпасы) и веществ (наркотические средства и психотропные вещества) и т.д. Иными словами, преступность уходит в глобальную цифровую среду.

В настоящее время современное цифровое пространство подвергается различным угрозам. Состояние его защищенности следует рассматривать как неотъемлемый элемент системы обеспечения национальной безопасности. Поэтому одним из актуальных вопросов современной науки является цифровая преступность. Многие ученые – специалисты в различных областях знаний, в частности в юриспруденции, занимаются исследованием сущности данного явления, выявлением причин и условий, способствующих его возникновению, разработкой мер, направленных на противодействие цифровой преступности.

Противодействие указанному криминальному явлению возможно при должной организации предварительного расследования преступлений, совершаемых в цифровом пространстве. Эффективность расследования уголовных дел о преступлениях, совершаемых в сфере цифровых технологий, как и всех иных видов преступных деяний, зависит от своевременности производства следственных действий. Как показывает практика, при расследовании цифровых преступлений правоохранительные органы нередко

сталкиваются с ситуацией, когда следственные действия должны быть проведены незамедлительно, то есть возникают случаи, не терпящие отлагательства, при которых даже небольшое промедление в производстве тех или иных следственных действий может привести к негативным последствиям в виде утраты доказательств, что значительно препятствует установлению истины по делу и привлечению виновных к уголовной ответственности. В таких случаях большая ответственность ложится на следователей, дознавателей, принимающих процессуальное решение о производстве следственного действия в случаях, не терпящих отлагательств. С одной стороны, решение субъектов предварительного расследования о производстве следственного действия в случаях, не терпящих отлагательств, может быть подвергнуто обжалованию, что, в свою очередь, способно повлечь за собой негативные последствия в виде признания доказательств недопустимыми и прекращению уголовного дела, а также привлечению к дисциплинарной ответственности. С другой, отказ от производства неотложных следственных действий также может привести аналогичному результату (утрата следов преступления, дисциплинарная ответственность и т.д.). Поэтому, следователь, дознаватель, в целях недопущения вышеперечисленных последствий должны знать положения уголовно-процессуального законодательства, регламентирующих вопросы производства следственных действий в случаях, не терпящих отлагательства, а также проанализировать материалы судебно-следственной практики, относящиеся к исследуемой теме.

Объектом исследования выступают общественные отношения, складывающиеся при производстве следственных действий в случаях нетерпящих отлагательства по уголовным делам о преступлениях, совершенных в сфере цифровых технологий.

Предметом исследования являются уголовно-правовая характеристика преступлений, совершенных в сфере цифровых технологий, общие положения уголовно-процессуального законодательства о производстве следственных действий в случаях, не терпящих отлагательства, а также особенности

производства следственных действий в случаях нетерпящих отлагательства по уголовным делам о преступлениях, совершенных в сфере цифровых технологий

Цель работы заключается в комплексном исследовании вопросов производства следственных действий в случаях нетерпящих отлагательства по уголовным делам о преступлениях, совершенных в сфере цифровых технологий.

Задачи выпускной квалификационной работы:

- 1) определить виды преступлений, совершенных в сфере цифровых технологий;
- 2) дать характеристику составам преступлений, совершенных в сфере цифровых технологий;
- 3) раскрыть сущность понятия «случаи, не терпящие отлагательства»;
- 4) проанализировать положения уголовно-процессуального законодательства, регламентирующие вопросы производства следственных действий случаях, не терпящих отлагательства;
- 5) рассмотреть процедуру расследования уголовных дел о преступлениях, совершенных в сфере цифровых технологий
- 6) выявить особенности производства отдельных следственных действий в случаях, не терпящих отлагательства и проанализировать материалы судебно-следственной практики.

Теоретическая основа исследования. При написании работы использованы труды отечественных и зарубежных ученых, исследовавших вопросы производства следственных действий в случаях нетерпящих отлагательства по уголовным делам о преступлениях, совершенных в сфере цифровых технологий среди них такие, как: как Е.С. Алексеева, И.В. Глазунова, П.А. Кудрявцев, А.В. Гриненко, А.Д. Назаров, К. Д. Лустач, Н.С. Манова, А. В. Огородник, И.В. Поляков и др.

Методологическая основа исследования представлена общенаучными методами познания, с помощью которых проведено исследование: диалектический метод, методы системного и сравнительного анализа. Использовались также такие частные научные методы, как формально-

юридический, сравнительно-правовой, историко-правовой, которые позволили рассмотреть явления в их взаимосвязи и взаимообусловленности.

Эмпирической основой исследования являлись различные статистические банки и сборники соответствующих подразделений правоохранительных органов, официально опубликованные материалы судебно-следственной практики, а также собственные наблюдения и практический опыт, полученный во время прохождения производственной (в том числе преддипломной) практики.

ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

§ 1. Понятие и виды преступлений, совершенных в сфере цифровых технологий

Для того, чтобы определить сущность и виды преступлений, совершенных в сфере цифровых технологий, необходимо исследовать само понятие цифровых технологий.

В отечественном законодательстве понятие «цифровые технологии» не закреплено. Данная категория может быть рассмотрена как технологии, позволяющие создавать, хранить, обрабатывать и распространять данные в электронном виде с использованием компьютера и компьютерных сетей (зачастую через Интернет)¹. При исследовании сущности преступлений в сфере цифровых технологий вполне закономерно возникает следующий вопрос: как соотносятся понятия информационные и цифровые технологии?

Информационные технологии являются более широкой категорией. Данное понятие охватывает все аспекты использования и управления информацией с помощью компьютерных систем и включается в себя такие компоненты, как разработка программного обеспечения, сетевая инфраструктура, хранение данных и т. д. Информационные технологии используются для обработки, передачи и хранения соответствующей информации.

Цифровые технологии могут быть рассмотрены как часть информационных технологий. В основе цифровых технологий также лежит информация, однако она представлена в электронной или цифровой форме. Он включает в себя такие аспекты, как использование цифровых устройств

¹ Цифровые технологии (в праве) [Электронный ресурс] // Большая российская энциклопедия URL: <https://bigenc.ru/c/tsifrovye-tekhnologii-v-prave-a80897> (дата обращения: 05.10.2023).

(компьютеры, смартфоны, планшеты), программного обеспечения, интернета, социальных сетей и других цифровых платформ.

Таким образом, информационные технологии являются более широким понятием, которое включает в себя все аспекты использования и управления информацией, тогда как цифровые технологии фокусируются на использовании лишь цифровой информации и технологий для решения соответствующих задач, и улучшения процессов.

При определении сущности и видов преступлений, совершенных в сфере цифровых технологий, будем придерживаться позиции И.В. Полякова, который выделяет две группы цифровых преступлений:

1) преступления, посягающие на цифровые технологии – ранее перечисленные цифровые платформы (цифровые устройства (компьютеры, смартфоны, планшеты), программное обеспечение, интернет, социальные сети и другие цифровые платформы);

2) преступления, совершаемые с использованием цифровых технологий¹.

К первой группе следует отнести преступления, закрепленные в Главе 28 УК РФ (Преступления в сфере компьютерной информации):

Статья 272. Неправомерный доступ к компьютерной информации.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности

¹ Поляков И.В. Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. – № 4. – 2020. – С. 21-25.

и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования.

Ко второй группе цифровых преступлений относятся преступные деяния, совершаемые с использованием цифровых технологий. Состав данных преступлений чаще всего характеризуется наличием такого квалифицирующего признака, как «использование электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет».

Отсутствие квалифицирующего признака в виде совершения преступления с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет не свидетельствует о том, что то или иное преступное деяние не может быть совершено с использованием цифровых технологий. Наоборот, цифровые технологии все чаще применяются для реализации преступных целей. В одних случаях цифровые технологии позволяют выполнить объективную сторону преступного деяния, к примеру, вымогательство с использованием сети Интернет, а в других – применяются для поиска соучастников, орудий преступления.

Так, в 2018 году был убит следователь по особо важным делам в транспортном управлении МВД по Центральному федеральному округу Евгения Шишкина. Предварительное расследование было завершено в 2020 году. Это стало первым раскрытым убийством, заказанным в «Даркнете».

Осужденный Абдулазизов согласился застрелить Шишкину с подачи несовершеннолетнего друга К.Г., который был координатором даркнет-магазина Los Zetas, торговавшего наркотиками. Г. познакомился с заказчиком убийства на платформе Hydra в даркнете. За то, чтобы «кое-кого убрать», Г. предложили миллион рублей. Получив все данные, Г. предложил это задание Абдулазизову, сказав, что «нужно убить нехорошую женщину». Тот согласился¹.

¹ Задержан организатор заказных убийств через даркнет [Электронный ресурс] // Российская газета URL: <https://rg.ru/2021/09/09/reg-pfo/zaderzhan-organizator-zakaznyh-ubijstv-cherez-darknet.html>(дата обращения 08.10.2023).

В данной выпускной квалификационной работе будут исследованы вопросы производства следственных действий, не терпящих отлагательств, по уголовным делам о преступлениях, в составах которых использование цифровых технологий выступает в качестве квалифицирующего признака, а также преступления, которые совершаются преимущественно с использованием цифровых технологий.

Преступные деяния, совершаемые с использованием цифровых технологий, могут быть разделены на несколько подгрупп в зависимости от видового объекта преступного посягательства:

1. Цифровые преступления против чести и достоинства личности.

К данной подгруппе цифровых преступлений относится клевета, ответственность за которую предусмотрена статьей 128.1 Уголовного кодекса. В части второй указанной статьи предусмотрен квалифицирующий признак – совершение клеветы публично с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет».

2. Цифровые преступления против собственности.

Данную группу преступлений в сфере цифровых технологий образуют такие деяния, закрепленные в Главе 21 УК РФ, как:

- Мошенничество (статья 159 УК РФ).
- Мошенничество с использованием электронных средств платежа (статья 159.3).
- Мошенничество в сфере компьютерной информации (статья 159.6).

3. Цифровые преступления, направленные против общественной безопасности. Это, в первую очередь, преступления террористической направленности, к примеру, публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма, заведомо ложные сообщения об акте терроризма, а также преступления, связанные с незаконным оборотом оружия и боеприпасов.

4. Цифровые преступления против здоровья населения. Это – преступления в сфере незаконного оборота наркотических средств и психотропных веществ.

5. Преступления против основ конституционного строя и безопасности государства. К данной группе цифровых преступлений следует отнести публичные призывы к осуществлению экстремистской деятельности (статья 280); возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (статья 282) и т.д.

Результаты исследований можно представить в виде схемы (Схема 1. Цифровые преступления и их виды).



§ 2. Характеристика составов преступлений, совершенных в сфере цифровых технологий

Рассмотрим составы преступлений, посягающих на цифровые технологии. Как было отмечено в предыдущем параграфе, к данной категории цифровых преступлений относятся уголовно-наказуемые деяния, закрепленные в Главе 28 УК РФ:

1. Статья 272. Неправомерный доступ к компьютерной информации.
2. Статья 273. Создание, использование и распространение вредоносных компьютерных программ.
3. Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
4. Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.
5. Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования.

Так как использование цифровых технологий относится к объективной стороне преступления, то в данной выпускной квалификационной работе основной акцент будет сделан на изучении объективных признаков состава цифровых преступлений.

Родовой объект исследуемых преступных деяний являются общественные отношения в области обеспечения общественной безопасности и охраны общественного порядка).

В качестве видового объекта компьютерных преступлений выступают общественные отношения, которые складываются в сфере обеспечения

конфиденциальности, целостности и доступности компьютерной информации, сохранности средств, используемых для её обработки.

Непосредственным объектом преступления, предусмотренного ст.272 являются отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями.

Предметом исследуемого преступления является охраняемая законом компьютерная информация.¹

Сущность компьютерной информации как предмета преступных посягательств раскрывается в примечании к ст. 272 УК РФ: «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Объективная сторона данного преступления складывается из:

- 1) действий, состоящих в неправомерном доступе к охраняемой законом компьютерной информации;
- 2) общественно-опасных последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации;
- 3) причинно-следственной связи между указанными действиями и последствиями.

Непосредственным объектом ст. 273 УК РФ являются общественные отношения, обеспечивающие безопасность в сфере компьютерной информации. Предмет данного преступления совпадает с предметом неправомерного доступа к компьютерной информации.

Статья 273 предусматривает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для

¹ Харламова А.А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации. Вестник Уральского юридического института МВД России. – № 2. – 2020. – С. 165.

несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, которые образуют объективную сторону исследуемого преступления.

Статья 274 УК РФ устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Данный состав преступления является материальным, так как обязательным условием для привлечения лица к уголовной ответственности является наступление таких альтернативных общественно-опасных последствий, как уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Непосредственный объект ст. 274 УК РФ совпадает с непосредственным объектом ст. 273 УК РФ. Предметом исследуемого вида преступления являются средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и окончное оборудование.

Статьей 274.1 УК РФ предусмотрена ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Критическая информационная инфраструктура, согласно Закону «О безопасности критической информационной инфраструктуры Российской Федерации» – это объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.¹

Объекты критической информационной инфраструктуры, согласно вышеназванному законодательному акту, – это информационные системы,

¹ О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г N 187 ФЗ - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 17.10.2023).

информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Неправомерное воздействие оказывается путем создания, распространения и (или) использование компьютерных программ либо иной компьютерной информации.

Создание компьютерных программ, как элемент объективной стороны преступных деяний, предусмотренных ст. 273, ст. 274.1 представляет собой действия, направленные на разработку, подготовку компьютерной программы, способствующей достижению преступных результатов, закрепленных в диспозициях ст. 273, ст. 274.1.

Распространение компьютерных программ предполагает предоставление доступа к ним любому постороннему лицу любым из возможных способов.

Использование программы - это работа с программой, применение ее по назначению и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме.

Далее рассмотрим преступления второй группы.

1. Цифровые преступления против чести и достоинства личности.

Использование цифровых технологий является способом совершения клеветы, сущность которой, как уголовно-наказуемого деяния, заключается в распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию (статья 128.1 УК РФ). Рассмотрим пример из материалов судебно-следственной практики.

Так, гражданин О. около двух лет встречался с девушкой по имени А. В день совершения преступления А. позвонила ему, и сказала, чтобы тот к нему больше не приходил, она живет с другим мужчиной. О. разозлился и решил отомстить А. следующим способом.

У фигуранта имелась страница в социальной сети Вконтакте. Далее О. переименовал свои данные, содержащиеся на странице, на данные А. (имя, фамилия, дата рождения). Далее О. загрузил с сети Интернет фотографию порнографического характера и определил её в качестве фотографии

пользователя, сделав надпись о том, что А. оказывает интимные услуги, и рядом указал её абонентский номер¹.

2. Преступления против собственности, которые совершаются с использованием цифровых технологий. Это, прежде всего, мошенничество.

Следует признать, что мошенничество является одним из самых динамичных преступлений современности, что выражается в постоянной разработке и применении новых способов и методов хищения чужого имущества.

Несмотря на то, что квалифицирующий признак в виде использования высоких технологий статьей 159 УК РФ не предусмотрен, объективная сторона мошенничества – обман или злоупотребление доверием – преимущественно совершается в цифровом пространстве. Для предоставления заведомо ложной, не соответствующей действительности информации преступники используют мессенджеры (преимущественно Телеграмм, способный обеспечивать анонимность), мобильные приложения, а также интернет-ресурсы (интернет-сайты).

Так, осужденный М. разместил в социальной сети «ВКонтакте» информацию розыгрыше электронной продукции компании «Apple». Далее он осуществил отбор из числа пользователей, заявивших о намерении участвовать в розыгрыше, лиц, в отношении которых будут совершаться мошеннические действия. После чего осужденным была организована переписка с вышеназванными пользователями, в ходе которой каждому из отобранных лиц М. направил сообщения с ложной информацией об их победе в розыгрыше и предложил оплату доставки мнимого приза путем зачисления денежных средств на лицевой счёт сообщённого им абонентского номера телефона².

¹ Приговор Чухломского районного суда Костромской области 02.05.2023 года по делу № 1-19/2023 [Электронный ресурс] // URL: <https://судебныерешения.рф/74195703/extended> (дата обращения: 25.10.2023).

² Приговор Великолукского городского суда (Псковская область) от 21 января 2020 года по делу № 1-18/2020 [Электронный ресурс]. URL: <https://sudact.ru/regular/doc/ReZKsD98lIx/> (дата обращения: 30.10.2023).

Нередко мошеннические действия совершаются в сфере компьютерной информации (статья 159.6 УК РФ). Мошенничество в сфере компьютерной информации представляет собой есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Приведу пример из материалов судебно-следственной практики.

Неустановленными в ходе следствия лицами был создан интернет-сайт, на котором размещено программное обеспечение, позволяющее удалённо управлять мобильными устройствами. Ссылка на сайт отправлена на абонентский номер гражданина К., который без каких-либо подозрений перешёл по ней. В результате действий К. без его ведома и согласия на его телефон было установлено вышеупомянутое программное обеспечение. Фигуранты получили возможность управлять смс-обменом, то есть, перехватывать входящие сообщения и отправлять от имени гражданина К. исходящие. Абонентский номер, находящийся в пользовании К., был подключён к сервису «Мобильный банк» Сбербанка. Для того, чтобы узнать количество денежных средств, фигуранты отправили запрос по номеру 900 и получили соответствующий ответ. После чего, воспользовавшись возможностью перевода денег через смс-сообщение, перечислили денежные средства, принадлежащие К. на другую банковскую карту, тем самым совершили хищение¹.

3. Цифровые преступления, направленные против общественной безопасности. В предыдущем параграфе было отмечено, что к данной категории цифровых преступлений относятся преступления террористической направленности, к примеру, публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или

¹ Постановление Рыбинского городского суда Ярославской области от 17.03.2023 по делу № 1-138/2023 [Электронный ресурс] // URL: <https://судебныерешения.рф/74493375/extended> (дата обращения: 04.11.2023).

пропаганда терроризма (статья 205.2), а также преступления, связанные с незаконным оборотом оружия и боеприпасов.

Следует признать, что террористическая деятельность давно осуществляется в цифровом пространстве, поэтому многие ученые и представители правоохранительных органов часто употребляют понятие «кибертерроризм». По мнению А.В. Огородника, «из-за высокого уровня развития техники террорист посредством подключенного к Интернету компьютера может нанести больший вред, чем различные взрывные устройства. Новые гаджеты рассматриваются преступниками, как средство для достижения целей, которые противоречат общепринятым морально-этическим нормам».¹

Так, в настоящее время распространение получили заведомо ложные сообщения об акте терроризма, которые осуществляются путем использования современных информационных технологий. Так, в последнее время распространение получили фейковые каналы в мессенджере Telegram, которые предоставляли пользователям сведения о будущих терактах на территории образовательных учреждений. Весной 2023 года на просторах «Телеграма» появился канал «Казанский Брейвик», автор которого обещал, что произойдут теракты в ТЦ «Московский», мечети «Ярдэм» и школе №70 города Казани. В ходе проверочных мероприятий указанная информация не нашла подтверждения².

Не менее актуальным является сообщение об акте терроризма путем отправления соответствующих сведений на электронную почту получателя.

Так, гражданин М. в вечернее время суток, находясь у себя дома, воспользовавшись сетью Интернет, нашел почтовый адрес городской больницы

¹ Огородник А. В. История возникновения кибертерроризма: от киберпреступности до кибертерроризма / А. В. Огородник // Донецкие чтения 2021: образование, наука, инновации, культура и вызовы современности: Материалы VI Международной научной конференции, Донецк, 26–28 октября 2021 года / Под общей редакцией С.В. Беспаловой. – Донецк: Донецкий национальный университет, 2021. С. 147.

² «Татарский маньяк» и «Казанский Брейвик» за фейки не ответят. [Электронный ресурс] // Вечерняя Казань | Дзен URL: https://dzen.ru/a/ZZ44sicKAQiquXp_ (дата обращения 09.11.2023).

и отправил сообщение о том, что территория больницы заминирована и скоро произойдет взрыв, если на киви-кошелек фигуранта не будут перечислены денежные средства в размере «данные изъяты». Также фигурантом предприняты меры, направленные на конспирацию преступной деятельности, а именно использовано приложение VPN, позволяющее менять IP-адрес устройства, с которого осуществлен выход в сеть.

Однако вышеназванное действие не позволило фигуранту сокрыть сведения о личности. В ходе оперативно-розыскных мероприятий установлено, что почтовый адрес, с которого получено сообщение об акте терроризма, привязан к абонентскому номеру, зарегистрированному на имя гражданина М. Далее сотрудниками уголовного розыска установлено местонахождение преступника, после чего фигурант был задержан¹.

Что касается незаконного оборота оружия и боеприпасов, то в качестве квалифицирующего признака данного преступного деяния законодатель устанавливает использование информационно-телекоммуникационных сетей, в том числе сети Интернет (п. «в» ч. 3 ст. 222 УК РФ).

Так, гражданин В., используя доступ к сети Интернет, с помощью сотового телефона осуществил вход в сеть Даркнет, где отыскал интернет-магазин, специализирующийся на продаже огнестрельного оружия. Осмотрев фотографии и пообщавшись с продавцом, принял решение о покупке огнестрельного оружия ПМ (Пистолет Макарова) и патронов к нему. Далее продавец отправил фигуранту координаты тайниковой закладки с оружием и боеприпасами. В. забрал оружие и боеприпасы. На следующий день, находясь рядом с отделом полиции, сделал два выстрела воздух и попытался скрыться, однако был задержан сотрудниками полиции².

¹ Приговор Советского районного суда г. Орел от 28.11.2022 по делу № 1-242/2022 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/72706234/extended> (дата обращения 09.11.2023).

² Приговор Воскресенского городского суда Московской области от 26.05.2022 по делу № 1-143/2022 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/66972674/extended> (дата обращения: 16.11.2023).

4. Цифровые преступления против здоровья населения. К данной разновидности цифровых преступлений отнесены преступления в сфере незаконного оборота наркотических средств и психотропных веществ. Так, деяние, предусмотренное статьей 228.1 УК РФ, содержит следующий квалифицирующий признак, относящийся к объективной стороне:

п. б) с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет).

По признаку, предусмотренному пунктом «б» части 2 статьи 228.1 УК РФ, при незаконном сбыте наркотических средств квалифицируются действия лица, которое с использованием сети Интернет подыскивает источник незаконного приобретения наркотических средств с целью последующего сбыта или соучастников незаконной деятельности по сбыту наркотических средств, а равно размещает информацию для приобретателей наркотических средств.

По указанному признаку квалифицируется и совершенное в соучастии преступление, если связь между соучастниками в ходе подготовки и совершения преступления обеспечивалась с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет (например, при незаконном сбыте наркотических средств обеспечивалась связь между лицом, осуществляющим закладку наркотических средств в тайники, и лицом, передавшим ему в этих целях наркотические средства).

Так, гражданин Б., являющийся пользователем мессенджера Телеграмм, откликнулся на предложение неустановленного лица, которое было связано с распространением наркотических средств на территории города Н. Неустановленное лицо пояснило, что сбыт наркотиков осуществляется бесконтактным способом – путем оборудования тайниковых закладок. Далее гражданин Б. направлен к куратору интернет-магазина, специализирующегося на продаже наркотиков. В ходе общения Б. объяснили суть работы, методы конспирации преступной деятельности, обсудили размер заработной платы и иные вопросы организационного характера.

Б. оборудовал тайниковые закладки, фотографировал их местоположение и отправлял соответствующие координаты с местоположением тайниковых закладок куратору¹.

5. Преступления против основ конституционного строя и безопасности государства. К данной группе цифровых преступлений следует отнести публичные призывы к осуществлению экстремистской деятельности (статья 280); возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (статья 282) и т.д.

В качестве примера рассмотрим статью УК РФ 280. Публичные призывы к осуществлению экстремистской деятельности. Объективная сторона данного преступления выражается в обращении к другим лицам с целью побудить их к осуществлению экстремистской деятельности. Преступная цель, как правило, достигается путем использования цифровых технологий.

Так, в одном из сообществ социальной сети ВКонтакте выложен пост с текстом: «В Израиле начались беспорядки из-за видео в TikTok». (Рисунок 1. Скриншот из сообщества «Голос Народа (НОВОСТИ РОССИИ)» в социальной сети ВКонтакте о массовых беспорядках в Израиле).

Гражданин Н., являющийся пользователем социальной сети «ВКонтакте» публично разместил под данную видеозапись адресованный неопределенному кругу лиц комментарий, призывающий к осуществлению насильственных действий в отношении группы лиц, выделенной по совокупности признаков религиозной и национальной принадлежности, доступный всем пользователям интернет-сайта².

¹ Приговор Кунгурского городского суда Пермского края от 30.08.2023 по делу № 1-420/2023 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/78050899/extended> (дата обращения: 21.11.2023).

² Приговор Ломоносовского районного суда г. Архангельск от 19.09.2023 по делу № 1-509/2023 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/77868426/extended> (дата обращения: 27.11.2023).

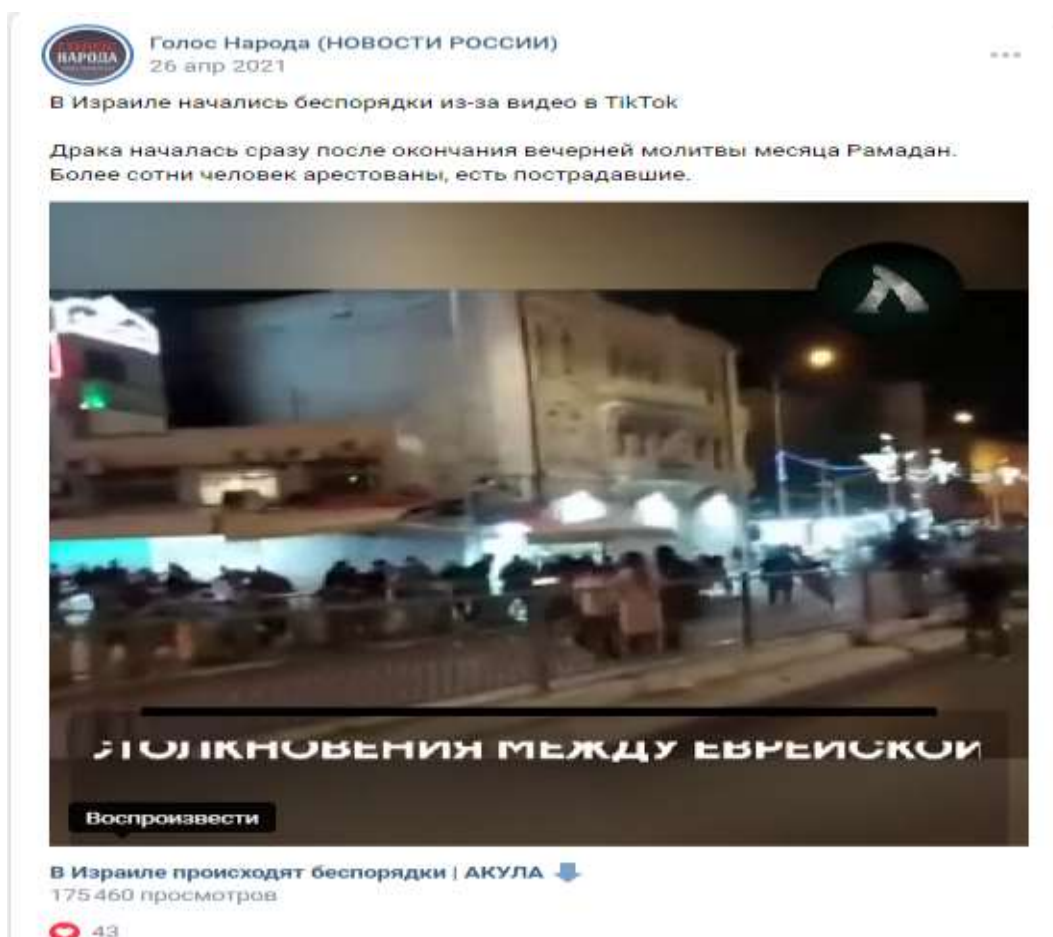


Рисунок 1. Скриншот из сообщества «Голос Народа (НОВОСТИ РОССИИ)» в социальной сети Вконтакте о массовых беспорядках в Израиле

Исследования, проведенные в рамках данной главы, позволяют сделать следующие выводы.

Группу цифровых преступлений образуют следующие уголовно-наказуемые деяния:

- преступления, посягающие на цифровые технологии – цифровые платформы (цифровые устройства (компьютеры, смартфоны, планшеты), программное обеспечение, интернет, социальные сети и другие цифровые платформы);
- преступления, совершаемые с использованием цифровых технологий.

Первая группа уголовно-наказуемых деяний связана с неправомерным доступом к компьютерной информации, созданием, использованием и распространением вредоносных программ, нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и

информационно-телекоммуникационных сетей, неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации, нарушением правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования. То есть, это преступления, закрепленные в Главе 28 УК РФ.

Вторую группу преступлений образуют деяния, объективная сторона которых реализуется путем использования цифровых технологий:

- преступления, направленные против чести и достоинства личности, в первую очередь, клевета;
- преступления, посягающие на отношения собственности, в частности, мошенничества и его отдельные виды;
- преступления, направленные против общественной безопасности (террористического характера, в сфере незаконного оборота оружия и боеприпасов);
- преступления против здоровья населения, преимущественно связанные с незаконным оборотом наркотических средств и психотропных веществ;
- преступления против основ конституционного строя и безопасности государства: публичные призывы к осуществлению экстремистской деятельности; возбуждение ненависти либо вражды, а равно унижение человеческого достоинства.

Состав данных преступлений, как правило, содержит такой квалифицирующий признак, как «использование электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет».

Помимо непосредственной реализации объективной стороны, цифровые технологии используются для поиска соучастников, орудий преступления.

ГЛАВА 2. ОБЩИЕ ПОЛОЖЕНИЯ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА О ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В СЛУЧАЯХ, НЕ ТЕРПЯЩИХ ОТЛАГАТЕЛЬСТВА

§ 1. Характеристика категории «случаи, не терпящие отлагательства» в уголовно-процессуальном законодательстве России

Производство следственных действий в случаях, не терпящих отлагательства, относится к актуальным вопросам современной уголовно-процессуальной науки. Так, в своих исследованиях Н.С. Манова отмечает, что исследуемая категория носит оценочный характер. По мнению автора, «неопределенность указанного термина вынуждает правоприменителя трактовать его содержание по личному усмотрению, вкладывать в него смысл, соответствующий их собственным представлениям. В ряде случаев это приводит к необоснованно ограничению прав и свобод участников уголовного судопроизводства». Также Н.С. Манова указывает на то, что «следственная ситуация может быть истолкована как не терпящая отлагательства, если существует реальная угроза утраты следов преступления или иных вещественных доказательств, продолжения преступной деятельности в случае промедления с производством следственного действия. Если следственное действие, требующее судебного решения, проводится без его получения в ситуации, не терпящей отлагательства, то в решении органа расследования о его производстве помимо указания на основания для производства соответствующего следственного действия должно быть обосновано наличие исключительной ситуации, делающей возможным вторжение в сферу охраняемых Конституцией РФ прав и интересов личности без разрешения суда.

То есть решение следователя (дознвателя) о производстве следственного действия должно содержать чёткое обоснование его безотлагательности»¹.

Е.С. Алексеева также акцентирует внимание на аналогичной проблеме. По мнению автора, «несмотря на употребление в тексте УПК рассматриваемого термина, законодатель не закрепляет его дефиниции. Между тем, именно неопределённость содержания данного понятия порождает трудности в практической деятельности, связанные, в частности, с последующей легализацией следственных действий, проведённых без судебных решений, а также с оспариванием стороной защиты законности производства следственных действий в ночное время»².

Согласно мнению А.Д. Назарова, А.И Баянов., В.А. Мажинского, «понятие «случаи, не терпящие отлагательства» является оценочным и в каждой конкретной ситуации следователь, дознаватель, принимая решение о применении нормы права, позволяющей отклониться от установленного общего процессуального порядка производства следственного действия (произвести его в ночное время либо без судебного решения, когда необходимость получения такого решения предусмотрена законом), на основе внутреннего убеждения определяет, является тот либо иной случай не терпящим отлагательства или не является таковым»³.

Помимо «производства следственных действий в случаях, не терпящих отлагательства», в действующем уголовно-процессуальном законодательстве содержится схожая по смыслу и содержанию категория - неотложные следственные действия.

¹ Манова Н.С. «Ситуация, не терпящая отлагательства» как оценочная категория в законодательстве и практике уголовного судопроизводства. Legal Concept, – 2019. – №18 (2), С. 42-48.

² Алексеева Е.С. Категория «Случаи, не терпящие отлагательства» в уголовно-процессуальном законодательстве и правоприменительной практике. Вестник Санкт-Петербургского университета МВД России. – 2019. – № (4 (84)). – С. 124-130.

³ Назаров А.Д., Баянов А.И., Мажинский В.А.. О целесообразности проведения следственных действий, предполагающих получение показаний, в ночное время при наличии случаев, не терпящих отлагательства. Вестник Сибирского юридического института МВД России. – 2021. – № (4 (45)), С. 190-196.

В отличие от случаев, не терпящих отлагательства, понятие «неотложные следственные действия» имеет законодательную дефиницию, которая содержится в п. 19 ст. 5 действующего УПК РФ:

- неотложные следственные действия - действия, осуществляемые органом дознания после возбуждения уголовного дела, по которому производство предварительного следствия обязательно, в целях обнаружения и фиксации следов преступления, а также доказательств, требующих незамедлительного закрепления, изъятия и исследования.

Как и случаи, не терпящие отлагательства, неотложные следственные действия являются объектом исследования отечественных ученых – специалистов в области уголовно-процессуального права. Так, по мнению Н.Г. Шурухнова, «сущность неотложных следственных действий (правового института) как особой процессуальной категории состоит в безотлагательности, направленности на поиск, обнаружение, исследование, закрепление следов совершенного преступления, получение и сохранение вещественных доказательств. Сведения, полученные при их проведении, являются базовыми для дальнейшего расследования, изобличения виновных, установления свидетелей, материального ущерба, выяснения других обстоятельств совершенного преступления»¹.

Согласно мнению К.Д. Лустача, «признак неотложности подразумевает следующее. Во-первых, у лица, ведущего уголовный процесс, есть обязанность (а не право) производить неотложные следственные действия, которая продиктована характерным для досудебного производства принципом публичности уголовного процесса. Во-вторых, неотложные следственные действия должны быть произведены ранее всех остальных, не требующих оперативного реагирования»².

¹ Шурухнов Н. Г. Качество неотложных следственных действий как необходимое условие эффективности расследования: к проблеме использования информационных технологий / Н. Г. Шурухнов // Российский следователь. – 2020. – № 8. – С. 18-22.

² Лустач, К. Д. Неотложные следственные действия: понятие и проблемы правового регулирования / К. Д. Лустач // Альманах молодого исследователя. – 2022. – № 12. – С. 99-103.

Вышеизложенное позволяет сделать вывод о том, что исследуемые уголовно-процессуальные категории могут быть рассмотрены как синонимы. Более того, в ходе прохождения преддипломной (производственной) практики установлено, что действующие следователи, дознавателем, а также оперативные работники в своей служебной деятельности оперируют понятиями «неотложный обыск», «неотложный осмотр», понимая под этим проведение соответствующих мероприятий в целях обнаружения и изъятия предметов, документов, имеющих значение дела, когда существующая следственная ситуация не терпит отлагательства. То есть, практические работники не видят существенную разницу между указанными уголовно-процессуальными категориями. В связи с вышеизложенным, считаю целесообразным исследование в рамках следующего параграфа положений УПК РФ, регламентирующих вопросы производства неотложных следственных действий.

Несмотря на то, что в законодательстве не содержится перечень случаев, не терпящих отлагательства, данный вопрос нашел отражение в актах Верховного суда РФ, а именно в Постановлении Пленума Верховного Суда РФ от 01.06.2017 № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)»¹. В пункте 16 исследуемого правового акта закреплено положение, согласно которому, к исключительным случаям, в которых производство следственного действия не могло быть отложено, относятся, например, ситуации, когда:

- необходимо реализовать меры по предотвращению или пресечению преступления;
- промедление с производством следственного действия позволит подозреваемому скрыться;

¹ О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ): Постановление Пленума Верховного Суда РФ от 01.06.2017 № 19 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 25.12.2023)

- возникла реальная угроза уничтожения или сокрытия предметов, или орудий преступления;

- имеются достаточные основания полагать, что лицо, находящееся в помещении или ином месте, в котором производится какое-либо следственное действие, скрывает при себе предметы или документы, могущие иметь значение для уголовного дела.

Перечень случаев, не терпящих отлагательства, содержится в нормативно-правовых актах органов, реализующих уголовно-процессуальные функции. Так, в целях установления единообразного порядка организации предварительного расследования в Следственном комитете Российской Федерации принят Приказ Следственного комитета РФ от 15.01.2011 № 2 «Об организации предварительного расследования в Следственном комитете Российской Федерации». Пунктом 1.9 Приказа, к случаям, не терпящим отлагательства, отнесены:

- а) необходимо реализовать меры по предотвращению, пресечению преступления, закреплению его следов;

- б) фактические основания для производства указанных следственных действий появились в ходе осмотра, обыска и выемки в другом месте;

- в) промедление с их производством позволит подозреваемому скрыться;

- г) неотложность их проведения обусловлена обстановкой только что совершенного преступления;

- д) возникла реальная угроза уничтожения или сокрытия искомых объектов;

- е) имеются достаточные основания полагать, что лицо, находящееся в помещении или ином месте, в котором производятся какие-либо следственные действия, скрывает при себе предметы или документы, могущие иметь значение для уголовного дела.

Таким образом, случаи, не терпящие отлагательства – это конкретные следственные ситуации, требующие немедленного, незамедлительного производства следственного действия в целях своевременного обнаружения и

изъятия доказательств по делу, пресечения противоправной деятельности. Данная категория является оценочной, поэтому следователь, дознаватель, орган дознания самостоятельно дают оценку возникшей обстановке и принимают решение о том, относятся ли сложившиеся условия к ситуациям, не терпящим отлагательства либо нет.

§ 2. Характеристика положений уголовно-процессуального законодательства, регламентирующих вопросы производства следственных действий случаях, не терпящих отлагательства

Проанализируем положения уголовно-процессуального законодательства, в которых содержится понятие «условия, не терпящие отлагательства».

Так, согласно части 3 статьи 164 УПК РФ производство следственного действия в ночное время не допускается, за исключением случаев, не терпящих отлагательства. Рассмотрим пример из материалов судебно-следственной практики.

Гражданин П. совершил разбойное нападение в отношении гражданина С. при следующих обстоятельствах.

Согласно материалам уголовного дела, фигурант находился в состоянии алкогольного опьянения в квартире, потерпевшего С., который являлся его знакомым. В ходе общения П. потребовал у С. передать ему немного денег для приобретения спиртных напитков, на что потерпевший ответил отказом. Далее у фигуранта возник умысел на совершение разбойного нападения.

Для того, чтобы исключить возможность оказания сопротивления гражданином С. при хищении денежных средств, фигурант нанес несколько ударов в голову потерпевшего, от которых тот упал и потерял сознание. Убедившись в том, что препятствия к хищению денежных средств полностью устранены, П. решил осмотреть одежду С., так как знал, что денежные средства тот носит в карманах брюк, и обнаружил денежные средства в размере 3200

рублей и похитил их. Помимо денег, фигурант также похитил сотовый телефон марки «Нокиа» и скрылся из квартиры.

Далее гражданин С. заявил о факте совершенного в отношении него преступления в местный отдел полиции, указал сведения о личности преступника и его возможное местонахождение. В рамках проведенных проверочных мероприятий преступник был задержан и доставлен в отдел полиции.

Далее, в ходе допроса фигурант сообщил, что денежные средства, которые похитил у потерпевшего, он потратил, однако сотовый телефон находится у него дома. Получив указанную информацию, следователем принято решение о производстве обыска, несмотря на ночное время.

Далее был осуществлен выезд к месту проживания фигуранта, проведен обыск, в ходе которого изъят сотовый телефон, являющийся предметом преступления и доказательством по уголовному делу. Действия следователя признаны правомерными, так как замедление в проведении указанного следственного действия могло привести к утрате вещественного доказательства¹.

Проведение следственных действий, которые носят поисковый характер в ночное время является вполне обоснованным решением. Возникает вопрос: следует ли распространять норму, закрепленную в части 3 статьи 164 УПК РФ на группу следственных действий, преследующих цель в виде получения показаний – допрос, очная ставка, проверка показаний на месте?

Считаю, что при принятии решения, предоставляющего субъектам предварительного расследования право на проведение следственного действия в ночное время суток, законодателем не учтен один важный момент. Дело в том, что при производстве осмотра, обыска и выемки объектом воздействия становится материальная среда, а при допросе, проверке показаний и очной ставке – человек и его сознание. Материальная среда (место происшествия, место

¹ Приговор Ленинского районного суда г. Кирова (Кировская область) № 1-255/2020 от 17 апреля 2020 г. по делу № 1-255/2020 33. - [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/QE4e5xM6l66T/> (дата обращения: 08.01.2024).

обыска, место проведения следственного эксперимента) является относительно устойчивым объектом. Все изменения, происходящие в материальной среде, носят объективный характер и не зависят от суточной цикличности. Информационное содержание материальной обстановки не меняется от времени суток (утро, день, ночь). Меняться может только качество полученного результата (осмотра, обыска и т.п.), так как в ночное время суток снижается работоспособность участников следственных действий и ухудшаются внешние условия, необходимые для нормальной работы со следами преступления.

Совершенно иными характеристиками обладает человек. Сознание человека в ночное время по причине снижением активности процессов жизнедеятельности становится уязвимым, не способным не только адекватно реагировать на внешние воздействия, но и противостоять им. В таком состоянии человек не может сознательно и свободно от внешнего воздействия проявлять волю и, соответственно, выражать свои мысли. Состояние сознания человека в ночное время не способствует получению полных и правдивых показаний. Нельзя исключать, что показания, полученные в ночное время, могут быть неполными, несвязными и даже ложными и не соответствовать содержанию информации, хранящейся в памяти допрашиваемого лица.

Однако нецелесообразность проведения следственных действий, направленных на получение показаний, в ночное время нельзя рассматривать в качестве препятствия для решения тех неотложных задач, которые могут быть решены только посредством получения показаний у отдельных лиц. Допрос не является единственным способом получения показаний. Информация, имеющая существенное значение для хода и направления расследования может быть получена путем производства оперативно-розыскного мероприятия «Опрос», который носит более упрощенный характер и не имеет процессуальные рамки.

В связи с вышеизложенным предлагается сформулировать ч.3 ст. 164 УПК РФ следующим образом:

- В ночное время недопустимо производство допроса, очной ставки, проверки показаний на месте, предъявления для опознания. Иные следственные действия могут быть проведены в случаях, не терпящих отлагательства.

В статье 165 содержатся нормы, определяющие судебный порядок получения разрешения на производство следственного действия. По общему правилу, следственные действия, ограничивающие конституционные права граждан, проводятся на основании судебного решения. Однако законодателем предусмотрена возможность производства указанной категории следственных действий без предварительного получения судебной санкции. Основанием является наличие исключительных случаев, не терпящих отлагательства.

В статье 179 УПК РФ регламентированы вопросы производства освидетельствования, сущность которого заключается в принудительном обследовании подозреваемого, обвиняемого, потерпевшего, а также свидетеля с его согласия в целях обнаружения на теле человека особых примет, следов преступления, телесных повреждений, выявления состояния опьянения или иных свойств и признаков, имеющих значение для уголовного дела. По общему правилу, данное следственное действие проводится после возбуждения уголовного дела, однако законодатель допускает производство освидетельствования до принятия указанного процессуального решения.

Следует согласиться с мнением И.В. Глазуновой и П.А. Кудрявцева о том, что «освидетельствование чаще всего носит неотложный характер, так как промедление с его производством может привести к утрате доказательств вследствие преднамеренных или неосторожных действий лица, подлежащего освидетельствованию»¹.

Производство освидетельствования в неотложном порядке, исходя из целей проведения данного следственного действия, имеет существенное значение для расследования и раскрытия уголовных дел о преступлениях,

¹ Глазунова И.В., Кудрявцев П.А. Освидетельствование как способ обнаружения и фиксации следов при расследовании преступлений. Вестник Российской таможенной академии. – 2017. – № 2. – С. 64-71.

посягающих на жизнь и здоровье граждан (причинение вреда здоровью, изнасилование и т.д.), а также о преступлениях, в составах которых нахождение в состоянии опьянения закреплено в качестве квалифицирующего признака.

Как было отмечено в предыдущем параграфе, в отечественном уголовно-процессуальном законодательстве содержится понятие «производство неотложных следственных действий», которое рассматривается в качестве синонима производства следственных действий в случаях, нетерпящих отлагательства.

Легальное, то есть законодательное определение понятия неотложных следственных действий содержится в действующем Уголовно-процессуальном кодексе РФ. В статье 5 УПК, где закреплены дефиниции базовых уголовно-процессуальных понятий, имеется следующее определение:

неотложные следственные действия - действия, осуществляемые органом дознания после возбуждения уголовного дела, по которому производство предварительного следствия обязательно, в целях обнаружения и фиксации следов преступления, а также доказательств, требующих незамедлительного закрепления, изъятия и исследования (п. 19 ст. 5 УПК РФ).

Следует признать, что определение, содержащееся в статье 5 УПК, носит узкий характер. Дело в том, что законодатель, сформулировав вышеназванную дефиницию, отнес к неотложным следственным действиям только те действия, которые проводятся после возбуждения уголовного дела и только органом дознания. В то же время на практике неотложный характер имеют, к примеру, осмотр места происшествия, производство экспертизы, то есть те следственные действия, которые проводятся до возбуждения уголовного дела, производство которых позволяет обнаружить и зафиксировать следы преступления и иные доказательства.

Неотложными являются и следственные действия, проводимые следователем и дознавателем. В статье 152 УПК РФ, регламентирующей вопросы, связанные с определением места проведения предварительного расследования, указано, что следователь, дознаватель, установив, что уголовное

дело ему не подследственно, производят неотложные следственные действия, после чего следователь передает уголовное дело руководителю следственного органа, а дознаватель - прокурору для направления по подследственности. То есть, субъектом проведения неотложных следственных действий является не только орган дознания, но дознаватель и следователь.

Правила производства неотложных следственных действий органами дознания можно определить путем анализа содержания дефиниции самого понятия неотложных следственных действий, а также уголовно-процессуальных норм, закрепленных в статье 157 УПК РФ.

Итак, рассмотрим первое правило производства неотложных следственных действий органами дознания, содержащееся в УПК РФ – указанная категория следственных действий проводится только органами дознания. Органы дознания – государственные органы и должностные лица, уполномоченные в соответствии с УПК РФ осуществлять дознание и другие процессуальные полномочия.

В части 2 статьи 157 УПК РФ указано, что неотложные следственные действия производят:

- 1) органы внутренних дел;
- 2) органы федеральной службы безопасности;
- 3) таможенные органы;
- 4) начальники органов военной полиции Вооруженных Сил Российской Федерации, командиры воинских частей, соединений, начальники военных учреждений и гарнизонов;
- 5) начальники учреждений и органов уголовно-исполнительной системы;
- 6) иные должностные лица, которым предоставлены полномочия органов дознания в соответствии со статьей 40 УПК РФ.

В статье 40 УПК РФ, которая определяет процессуальный статус органов дознания, закреплено правило, согласно которому возбуждение уголовного дела и выполнение неотложных следственных действий возлагаются также на:

1) капитанов морских и речных судов, находящихся в дальнем плавании, - по уголовным делам о преступлениях, совершенных на данных судах;

2) руководителей геологоразведочных партий и зимовок, начальников российских антарктических станций и сезонных полевых баз, удаленных от мест расположения органов дознания, указанных в части первой настоящей статьи, - по уголовным делам о преступлениях, совершенных по месту нахождения этих партий, зимовок, станций, сезонных полевых баз;

3) глав дипломатических представительств и консульских учреждений Российской Федерации - по уголовным делам о преступлениях, совершенных в пределах территорий данных представительств и учреждений.

Таким образом, неотложные следственные действия могут проводить не только органы и должностные лица, напрямую относящиеся к органам дознания, но и другие субъекты уголовно-процессуальных отношений, которые при определенных случаях обязаны провести соответствующие неотложные мероприятия.

В уголовно-процессуальном законодательстве содержится норма, согласно которой, следователь, дознаватель, установив, что уголовное дело ему не подследственно, производит неотложные следственные действия, после чего следователь передает уголовное дело руководителю следственного органа, а дознаватель - прокурору для направления по подследственности (часть 5 статьи 152 УПК РФ).

То есть, имеет место противоречие между статьей 157 и статьей 152 УПК РФ, так как первая предполагает производство следственных действий неотложного характера только органами дознания, а вторая – следователем и дознавателем. В целях исключения данного противоречия, в статье 5 УПК РФ следует указать на возможность производства неотложных следственных действий следователем и дознавателем.

Второе правило – неотложные следственные действия проводятся по делам о преступлениях, по которым производство предварительного следствия обязательно. В данном случае необходимо применить положения уголовно-

процессуального законодательства, определяющие подследственность уголовных дел. Согласно мнению А.В. Гриненко, «подследственность представляет собой совокупность правил, применение которых позволяет отнести то либо иное уголовное дело к компетенции конкретного следователя или дознавателя»¹.

В статье 151 УПК РФ закреплён перечень должностных лиц, уполномоченных на производство предварительного следствия, и перечень статей Уголовного закона, по которым производство следствия обязательно.

Органы внутренних дел осуществляют производство неотложных следственных действий по всем уголовным делам, за исключением тех, которые относятся к компетенции органов федеральной службы безопасности, таможенных органов, органов уголовно-исполнительной системы и т.д. Органы федеральной службы безопасности проводят неотложные следственные действия по уголовным делам о преступлениях, подследственных следователям данной службы. Таможенные органы - по уголовным делам о преступлениях, предусмотренных статьями 173.1, 173.2, 174, 174.1, 189, 190, 193 частью второй, 193.1 частями второй и третьей, 194 частями третьей и четвертой, 200.1 частью второй, 200.2 частями второй и третьей, 226.1, 229.1 Уголовного кодекса Российской Федерации, выявленных таможенными органами.

Однако, необходимость в неотложном производстве следственных действий возникает не только по уголовным делам о преступлениях, по которым производство следствия обязательно. Дознаватель, органы дознания также могут провести неотложные следственные действия по уголовным делам, по которым предусмотрено производство дознания.

Следующее правило – неотложные следственные действия проводятся после возбуждения уголовного дела, то есть их производство возможно только в рамках возбужденного уголовного дела, а не после получения заявления

¹ Гриненко А. В. Уголовный процесс: учебник и практикум для среднего профессионального образования / А. В. Гриненко. — 9-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. С. 171.

(сообщения) о преступлении. Однако в предыдущих параграфах было указано, что определение понятия неотложных следственных действий необходимо расширить и внести соответствующие изменения в пункт 19 статьи 5 УПК РФ.

Конкретные правила уголовно-процессуального законодательства распространяются и на последующую деятельность субъектов производства неотложных следственных действий. Орган дознания, проводившие неотложные следственные действия, не позднее 10 суток со дня возбуждения уголовного дела направляет уголовное дело руководителю следственного органа в соответствии с пунктом 3 статьи 149 УПК РФ.

В тех случаях, когда неотложные следственные действия проводят следователь, дознаватель, то применяются положения Уголовно-процессуального кодекса, закрепленные в части 5 статьи 152.

После направления уголовного дела руководителю следственного органа орган дознания может производить по нему следственные действия и оперативно-розыскные мероприятия только по поручению следователя. В случае направления руководителю следственного органа уголовного дела, по которому не обнаружено лицо, совершившее преступление, орган дознания обязан принимать розыскные и оперативно-розыскные меры для установления лица, совершившего преступление, уведомляя следователя об их результатах. Следователь, дознаватель как субъекты производства неотложных следственных действий, вышеуказанными обязанностями не наделены.

На основании вышеизложенного можно сделать следующие выводы.

Случаи, не терпящие отлагательства – это конкретные следственные ситуации, требующие немедленного, незамедлительного производства следственного действия в целях своевременного обнаружения и изъятия доказательств по делу, пресечения противоправной деятельности. Ситуации, относящиеся к категории не терпящих отлагательства, определены в Постановлении Пленума Верховного суда РФ и в некоторых ведомственных нормативно-правовых актах:

- необходимо реализовать меры по предотвращению или пресечению преступления;
- промедление с производством следственного действия позволит подозреваемому скрыться;
- возникла реальная угроза уничтожения или сокрытия предметов, или орудий преступления;
- имеются достаточные основания полагать, что лицо, находящееся в помещении или ином месте, в котором производится какое-либо следственное действие, скрывает при себе предметы или документы, могущие иметь значение для уголовного дела.

В части 3 статьи 164 УПК РФ установлен законодательный запрет на производство следственного действия в ночное время, за исключением случаев, не терпящих отлагательства.

В статье 165 закреплены нормы, определяющие судебный порядок получения разрешения на производство следственных действий, ограничивающих конституционные права граждан. При наличии исключительных случаев, не терпящих отлагательства, производство указанной категории следственных действий возможно без предварительного получения судебной санкции.

В статье 179 УПК РФ регламентированы вопросы производства освидетельствования. По общему правилу, данное следственное действие проводится после возбуждения уголовного дела, однако законодатель допускает производство освидетельствования до принятия указанного процессуального решения.

Неотложные следственные действия представляют собой действия, проводимые следователем, дознавателем, органом дознания в целях обнаружения и фиксации следов преступления, а также доказательств, требующих незамедлительного закрепления, изъятия и исследования.

Субъектами производства неотложных следственных действий выступают следователь, дознаватель, орган дознания. Требования уголовно-

процессуального законодательства, связанные с производством неотложных следственных действий, также распространяются на должностных лиц, перечисленных в статье 40 УПК РФ: капитаны морских и речных судов, руководители геологоразведочных партий и зимовок, глав дипломатических представительств. Конкретные правила уголовно-процессуального законодательства распространяются и на последующую деятельность субъектов производства неотложных следственных действий. Орган дознания, проводившие неотложные следственные действия, не позднее 10 суток со дня возбуждения уголовного дела направляет уголовное дело руководителю следственного органа в соответствии с пунктом 3 статьи 149 УПК РФ.

ГЛАВА 3. ОСОБЕННОСТИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В СЛУЧАЯХ НЕТЕРПЯЩИХ ОТЛАГАТЕЛЬСТВА ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

§ 1. Характеристика процедуры расследования уголовных дел о преступлениях, совершенных в сфере цифровых технологий

Рассмотрим процесс расследования преступлений, совершаемых в сфере цифровых технологий.

Уголовные дела о преступлениях, закрепленных в Главе 28 УК РФ (Преступления в сфере компьютерной информации), посягающих на цифровые технологии, как правило, возбуждаются на основании заявления (сообщения) о преступлении. Согласно положениям действующего уголовно-процессуального законодательства, перед принятием решения о возбуждении уголовного дела организуется и проводится проверка сообщения о преступлении. В рамках проверочных мероприятий проводится опрос заявителя, в ходе которого устанавливается событие преступления, то есть, время, место, способ его совершения. Следует отметить, что уголовные дела об исследуемой категории преступных деяний возбуждаются по факту совершенного преступления, то есть, органы предварительного расследования в большинстве случаев не обладают сведениями о личности подозреваемого. Проанализируем пример из материалов судебно-следственной практики.

Гражданка Л. занимала должность специалиста офиса продаж компании «Х», которая предоставляет телекоммуникационные услуги, и имела доступ к базам данных организации, в которых хранилась информация о персональных данных клиентов. Далее в мессенджере «Telegram» к ней обратились неустановленные лица, и предложили материальное вознаграждение в размере 500 рублей за предоставление персональных данных каждого клиента, на что

фигурант ответил согласием. Л. фотографировала персональные данные клиента, интересовавшего неустановленных лиц, и отправляла фотографии посредством мессенджера «Телеграмм». Для достижения преступных целей фигурант использовал мобильный телефон «iPhone 11». Согласно правовым актам организации «Х», обращение к персональным данным клиентов допускалось при их присутствии либо на основании нотариально заверенной доверенности от абонента.

Факт незаконного обращения к персональным данным был выявлен сотрудниками службы безопасности, после чего информация поступила в правоохранительные органы.

Получив данную информацию, сотрудниками УФСБ был осуществлен выезд на место происшествия. Гражданке «Л» предложено выдать технические средства, принадлежащие ей и имеющие отношение к преступной деятельности. Л. выдала оперативным сотрудникам сотовый телефон «iPhone 11». В ходе осмотра сотового телефона обнаружена переписка в мессенджере «Телеграмм» с неустановленными лицами. Также в ходе осмотра были определены лица, персональные данные которых были переданы неустановленным лицам за денежное вознаграждение. Далее проведен их опрос, все опрашиваемые лица пояснили, что в организацию «Х» с требованием о предоставлении персональных данных они не обращались, доверенность не составляли.

В рамках производства по уголовному делу осуществлено изъятие видеозаписи с камеры видеонаблюдения, расположенного рядом с рабочим местом гражданки Л. На видеозаписи запечатлена Л., производящая в помещении магазина манипуляции с рабочим компьютером и личным мобильным телефоном.

Далее осмотрено программное обеспечение, которое позволяет получить доступ к персональным данным клиентов. В ходе осмотра установлены дата, время и содержание запросов, осуществленных Л (поиск абонента по абонентскому номеру, результатом которого является отображение соответствующей карточки абонента).

В ходе расследования уголовного дела получены кадровые документы, которые свидетельствуют о том, что фигурант действительно выполнял функции, связанные с оказанием телекоммуникационных услуг, имел доступ к соответствующим базам данных и был предупрежден об ответственности за действия, связанные с неправомерным доступом:

- копия приказа о приеме работника на работу с приложениями обязательством о сохранении коммерческой тайны и иной конфиденциальной информации;
- копия подписки об ответственности за совершение противоправных действий;
- копия должностной инструкции специалиста офиса продаж¹.

Исходя из вышеизложенного примера из материалов судебно-следственной практики, процедуру расследования данной группы преступлений, совершаемых в сфере цифровых технологий, можно представить в следующем виде:

1) получение сообщения (заявления) о преступлении и осуществление проверочных мероприятий:

- опрос лица, в отношении которого поступило заявление;
- осмотр места происшествия и изъятие предметов (компьютерного и иного технического оборудования, видеозаписей и т.д.) документов, имеющих отношение к преступлению;
- осмотр изъятых предметов и документов;
- установление личности потерпевших и их опрос;
- запрос на представление кадровых документов (приказ о назначении на должность, должностная инструкция и т.д.);

2) возбуждение уголовного дела и производство предварительного расследования:

¹ Приговор Московского районного суда г. Калининград от 06.10.2023 по делу № 1-237/2023 33. - [Электронный ресурс]. – URL: <https://судебныерешения.рф/77116661/extended> (дата обращения: 26.01.2023).

- допрос всех участников – подозреваемого, потерпевшего, свидетелей;
- назначение экспертиз (компьютерной, дактилоскопической, портретной и т.д.).

- производство иных следственных действий в зависимости от характера совершенного преступления и полноты данных, полученных в ходе проверки сообщения о преступлении.

Процесс расследования цифровых преступлений против собственности имеет определённое сходство с расследованием компьютерных преступлений.

Уголовные дела о мошенничестве, относящегося к категории самых распространённых цифровых преступлений, возбуждаются на основании заявления потерпевшего. Аналогичный порядок имеет деятельность органов предварительного расследования и оперативных подразделений на этапе проверки сообщения о преступлении, на первоначальном и последующем этапах расследования.

Рассмотрим процедуру расследования цифровых преступлений имущественного характера на примере расследования и раскрытия мошенничества, совершенного на сайте Авито с использованием функции Авито-Доставка.

Так, с заявлением в дежурную часть отдела полиции "Х" обратился гражданин В. С просьбой привлечь к ответственности неизвестного ему лица, которое обманным путем завладело его денежными средствами.

По данному факту было организовано проведение мероприятий, направленных на проверку сообщения о преступлении.

В ходе опроса гражданин В. пояснил, что на сайте Авито хотел приобрести сотовый телефон "iPhone 7". В целях приобретения телефона написала неизвестному ему продавцу соответствующего мобильного устройства (в ходе расследования будет установлено, что им является гражданин Е.). Переписка осуществлялась на сайте Авито, а затем в мессенджере "Ватсап". На сайте был указан номер продавца.

Далее Е. предложил потерпевшему воспользоваться функцией «Авито. Доставка», на что В. согласился. Для оплаты товара Е. отправил ссылку, где необходимо было ввести данные банковской карты и подтвердить оплату. Потерпевший выполнил указания и перечислил требуемую сумму на банковскую карту. Получив денежные средства, Е. написал В. и сказал, что вечером отправит по почте, после чего телефон Е. был недоступен.

Далее следователем было принято решение о возбуждении уголовного дела. Гражданин В. допрошен в качестве потерпевшего. Следователем проведен осмотр сотового телефона потерпевшего, с которого осуществлялась покупка телефона "iPhone". В ходе осмотра получены:

- скриншоты переписки потерпевшего с фигурантом на сайте Авито;
- скриншоты переписки Е. и В. в мессенджере «Ватсап»;
- скриншоты с сайта Авито (само объявление о продаже сотового телефона);
- справки по операции банка «Тинькофф» (перевод денег на счёт подозреваемого).

Далее были проведены мероприятия, направленные на установление личности подозреваемого. Так, было установлено, что абонентским номером, с которого осуществлялась переписка в мессенджере Ватсап, принадлежит гражданину Е.

Далее принято решение о задержании Е. и проведении мероприятий в жилище задержанного в целях обнаружения и изъятия технических устройств, путем использования которых было совершено мошенничество. Следователем проведен допрос Е., который признал вину, а также осмотр жилища с согласия Е. В ходе осмотра изъят сотовый телефон, принадлежащий Е., с установленным приложением Авито, а также банковские карты, которые в последующем были осмотрены¹.

¹Постановление Нижнекамского городского суда (Республика Татарстан) от 28 мая 2020 года по делу № 1-245/2020. - [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/vDG8KdwkPKbO/> (дата обращения: 30.01.2024)

Таким образом, расследование цифрового мошенничества имеет следующую типичную процедуру:

1) опрос (допрос) лица в качестве потерпевшего, в ходе которого устанавливаются обстоятельства совершенного преступления (время, место, способы обмана, способы оплаты, размер причиненного вреда и т.д.);

2) осмотр сотового телефона, иного технического оборудования, с помощью которого велась переписка с преступником, осуществлен перевод денежных средств;

3) проведение мероприятий, направленных на установление личности и местонахождения подозреваемого.

Далее необходимо исследовать процедуру расследования цифровых преступлений, посягающих на общественный порядок и общественную безопасность. Как было отмечено в предыдущей главе, в настоящее время цифровые технологии широко используются в сфере незаконного оборота наркотиков. В отличие от мошенничества и компьютерных преступлений, уголовные дела по которым возбуждаются по факту их совершения, преступления в сфере незаконного оборота наркотиков выявляются сотрудниками оперативных, а также строевых подразделений (ППС, ДПС) в рамках оперативно-розыскных мероприятий либо повседневной служебной деятельности (ППС, ДПС). Как и в предыдущем случае, процесс расследования наркопреступлений, совершаемых с использованием цифровых технологий, будет рассмотрен на конкретном примере.

Так, гражданин И. обнаружил надпись на стене одного из многоквартирных домов о высокооплачиваемой работе и название канала в мессенджере «Телеграмм», тогда он, со своего мобильного телефона марки «Itel A17», написал администратору канала, данные которого не помнит. Администратор канала пояснил И., что работа заключается в оборудовании тайниковых закладок с наркотическими средствами на территории города Т. за денежное вознаграждение, на что И. ответил согласием.

После чего фигурант оплатил залог в размере 5000 рублей путем перевода денежных средств неустановленному лицу по реквизитам, предоставленным администратором канала, с помощью сервиса «Витара», и вступил в преступную связь с неустановленным лицом.

Далее И. поступило первое задание, согласно которому он должен был забрать наркотические средства из тайника и расфасовать их дома. Фигурант отыскал тайник с наркотическим средством, принес домой и осуществил расфасовку. В результате чего были получены свертки с наркотическим средством «мефедрон» с массой 1-2 грамма в каждом. Далее И. должен был разложить полученные свертки на безопасной территории.

В целях реализации преступных целей И. направился в лесной массив одного из районов города и стал оборудовать тайниковые закладки рядом с лесом. Вскоре фигурант был замечен сотрудниками полиции ППСП, находящимися на маршруте патрулирования. И в связи с тем, что И. вел себя подозрительно и постоянно оглядывался, при виде сотрудников полиции стал нервничать, было принято решение о его задержании. О факте задержания сообщено в дежурную часть ближайшего отдела полиции в целях обеспечения прибытия следственно-оперативной группы.

Далее в присутствии двух незаинтересованных лиц проведен личный досмотр гражданина И., в ходе которого обнаружены свертки с наркотическим средством «мефедрон». Далее задержанный И. предоставил телефон «iPhone 6», в ходе осмотра которого обнаружены фотоизображения с географическими координатами местоположения тайниковых закладок с наркотиками, оборудованными И. до задержания. После чего, сотрудниками СОГ в рамках осмотра места происшествия по координатам, имеющимся в сотовом телефоне, принадлежащем И., изъяты свертки с наркотическим средством «мефедрон».

И. в присутствии двух незаинтересованных лиц предложено пройти медицинское освидетельствование на состояние опьянения, на что задержанный ответил отказом¹.

Данный пример позволяет сделать вывод о том, что расследование преступлений, связанных с незаконным оборотом наркотиков имеет следующую процедуру.

1) задержание лица сотрудниками полиции и сообщение о данном факте в дежурную часть;

2) личный досмотр задержанного, осмотр телефона с разрешения фигуранта в целях отыскания фотоизображения с тайниковыми закладками для их дальнейшего изъятия СОГ;

3) изъятие наркотиков из тайниковых закладок, оборудованных задержанным ранее;

4) предложение пройти медицинское освидетельствование на состояние опьянения;

5) направление изъятых веществ и предметов на исследование;

6) после возбуждения уголовного дела проводятся допросы подозреваемого, свидетелей (сотрудников полиции, принимавших участие в задержании, незаинтересованных лиц, участвовавших при личном досмотре, осмотре места происшествия);

7) производство обыска по месту жительства (часто в качестве неотложного следственного действия);

8) проверка показаний на месте – на местах оборудования тайниковых закладок, проведение очных ставок и иных следственных и процессуальных действий в зависимости от сложившейся следственной ситуации.

Рассмотрим процедуру расследования преступлений экстремистской направленности, совершаемых с использованием цифровых технологий. Данные

¹ Приговор Октябрьского районного суда г. Ставрополя от 02.11.2023 по делу № 1-354/2023 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/78771438/extended> (дата обращения: 07.02.2024).

преступные деяния в большинстве случаев выявляются сотрудниками оперативных подразделений в рамках соответствующих оперативно-розыскных мероприятий. При получении информации, содержащей признаки экстремистской деятельности, осуществляемой с использованием цифровых технологий, устанавливаются:

- места неправомерного проникновения в компьютерные сети либо распространения запрещенных материалов, способы преодоления информационной защиты (подбор либо знание паролей, отключение средств защиты, использование несовершенств такой защиты, применение специальных программных средств);

- содержание и назначение информации, подвергшейся воздействию либо распространенной в интернете, ее отнесение к экстремистским материалам;

- средства, использованные при совершении противоправных действий (технические, программные, комбинированные);

- принадлежность IP-адресов и доменных имен.

В рамках проверки сообщения о преступлении и производства по уголовному делу проводятся следующие мероприятия:

- осмотр интернет-ресурсов, на котором были размещены материалы, возможно относящиеся к категории экстремистских;

- назначение судебной лингвистической экспертизы экстремистских материалов;

- истребование сведений из службы безопасности или администрации интернет-ресурса на предмет получения информации о пользователе, его регистрационных данных, IP-адресе, с которого им осуществляется доступ к ресурсу и был размещен тот или иной запрещенный материал. Как правило, реализуется в рамках отдельного поручения силами и средствами сотрудников оперативных подразделений, осуществляющих оперативно-розыскное обеспечение процесса расследования уголовного дела;

- истребование сведений у интернет-провайдера и оператора связи о конкретном абоненте, приобщить копию договора на оказание услуг связи;

- установление адреса помещения, откуда пользователь выходил в интернет при размещении запрещенного контента, получение характеризующих сведений на это лицо;
- осмотр (обыск) в помещении, где находится компьютерное, другое телекоммуникационное оборудование, обеспечивающее доступ в интернет, и их изъятие;
- допрос подозреваемого, обвиняемого, свидетелей.

Расследование преступлений террористической направленности, к примеру, публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма, совершаемых с использованием цифровых технологий, имеет сходство с процедурой расследования экстремизма. Аналогичные мероприятия проводятся в целях установления местоположения подозреваемого, компьютерного оборудования, путем использования которого совершено противоправное деяние.

§ 2. Производство отдельных следственных действий в случаях, не терпящих отлагательства. Обзор правоприменительной практики

Наиболее распространенным следственным действием, проводимым в условиях, не терпящих отлагательств, относится обыск (выемка).

Так, гражданин З. находился в федеральном розыске и скрывался в городе С. В связи с нахождением в розыске, З. не имел легального источника дохода, поэтому решил заняться преступной деятельностью, а именно мошенничеством в сфере компьютерной информации, что также сопровождалось неправомерным доступ к компьютерной информации, содержащейся в компьютерных системах организаций «Х» и «А».

В целях осуществления преступной деятельности, З. посредством сети Интернет изучил возможность хищения хранящихся на счетах безналичных

денежных средств, путём неправомерного доступа к охраняемой законом компьютерной информации посредством сети Интернет. Также З. был осведомлен о необходимости для совершения хищения наличия у похитителей большого количества банковских счетов и карт, а также сим-карт операторов связи, оформленных на лиц, достоверно неосведомленных об использовании их счетов и карт в преступных целях (далее подставных лиц), скорейшего вывода безналичных денежных средств с подконтрольных счетов, на которые они перечислены непосредственно при хищении, на другие подконтрольные счета и скорейшего их обналичивания во избежание отмены или блокирования операций при обнаружении хищения.

З. не владел техническими навыками, позволяющими осуществить неправомерный доступ к компьютерной информации, поэтому посредством мессенджера «Jabber» преступил в преступный сговор неустановленным лицом. Данное лицо выполняло функции, связанные с получением неправомерного доступа к компьютерной информации, принадлежащей организациям «Х» и «А». Согласно материалам уголовного дела, неустановленное лицо осуществило несанкционированную загрузку и установку программного обеспечения в персональные компьютеры организации «Х», в результате чего получен удаленный доступ, в том числе возможность получать снимки содержимого рабочего стола ПК, воспроизводить нажатие клавиш клавиатуры и движение указателя, а также удаленно управлять ПК «Х», повлекший модификацию и копирование компьютерной информации из корыстной заинтересованности. Далее, неустановленное лицо установило в ПК «Х» программное обеспечение «qiwicashier.exe», что позволило управлять (администрировать) счетом организации «Х» в платежной системе «QIWI» КИВИ Банк (АО) и беспрепятственно производить транзакции находящихся на указанном счете денежных средств.

Денежные средства организации «Х» зачислялись на «QIWI-кошельки», которые были зарегистрированы на абонентские номера лиц, не осведомленных о преступной деятельности. Подбор абонентских номеров осуществлял

гражданин Б., который также был вовлечен в организованную группу. Обналичивание похищенных денег также отнесено к функциям Б.

В ходе производства по делу, установлено местонахождение гражданина Б., и в соответствии с уголовно-процессуальным законодательством, принято решение о производстве неотложного обыска в его жилище. При обыске изъяты банковские карты, сим-карты различных операторов сотовой связи, Интернет-модемы «Йота», банковская документация, 6 ноутбуков различной модификации, 5 сотовых телефонов и другое имущество, принадлежащее Б.

Далее следователем проведено следственное действие – осмотр изъятого в ходе обыска ноутбука. При осмотре обнаружена программа «Jabber», в которой имеется переписка гражданина Б. с аккаунтом «данные изъяты». В рамках последующих оперативно-розыскных установлено, что данный аккаунт принадлежит гражданину З., который в последующем также был задержан¹.

В отличие от мошенничества, преступлений в сфере компьютерной информации, при расследовании преступных деяний, связанных с незаконным оборотом запрещенных веществ и предметов (наркотические средства и психотропные вещества, оружие и боеприпасы), неотложный обыск проводится в целях отыскания и изъятия указанных предметов и веществ.

Так, гражданин Г. посредством информационно-телекоммуникационной сети Интернет, в мессенджере «Телеграм» заказал у неустановленного лица наркотические средства «гашиш», «марихуана», «МДМА», а также психотропное вещество «амфетамин», которые в последующем хранил у себя дома для последующей перепродажи. Иными словами, фигурант открыл собственный магазин по продаже наркотиков.

Далее фигурант оборудовал два тайника с наркотиком, сфотографировал местность и с привязкой географических координат отправил их потребителю. После чего М. был задержан сотрудниками подразделения по контролю за

¹ Приговор Первомайского районного суда г. Краснодара от 19.07.2018 по делу № 1-50/2018 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/35324463/extended> (дата обращения: 27.02.2024).

оборотом наркотиков. Следственно-оперативной группой осуществлено изъятие двух свертков с наркотическим средством «гашиш», массой 0,29 и 1,89 грамма. В ходе беседы задержанный признался, что дома также имеются наркотические средства.

По данному факту следователем возбуждено уголовное дело и принято решение о производстве обыска в случаях, не терпящих отлагательства. Далее по месту жительства осуществлен выезд следственно-оперативной группы. В ходе обыска в жилище М. обнаружены и изъяты: сверток с наркотическим средством «гашиш», общей массой 191,3 грамма, сверток с наркотическим средством «МДМА», общей массой 150,1 грамма, сверток с психотропным веществом – амфетамин массой 25,1 грамма¹.

Помимо обыска (выемки), существенное значение для раскрытия и расследования преступлений, совершаемых с использованием цифровых технологий, относится осмотр предметов – технических средств, которые используются для достижения преступного результата.

Так, в ходе оперативно-розыскного мероприятия «Наблюдение» по подозрению сбыте наркотических средств задержан гражданин К. Путем производства личного досмотра фигуранта обнаружены и изъятые 15 свертков, содержащих в своем составе наркотическое средство.

В ходе общения с оперативными сотрудниками задержанный пояснил, что работает закладчиком наркотических средств в интернет-магазине, в его мобильном телефоне, находятся фотографии тайников (закладок) с наркотическими средствами, раскладку которых он осуществил. Фигурант открыл телефон и показал фотографии оборудованных им тайников. Далее, по

¹ Приговор Приволжского районного суда г. Казани (Республика Татарстан) от 24 июля 2019 г. по делу № 1-317/2019 - [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/Py1ROQJXQWq/> (дата обращения: 28.02.2024).

координатам, указанным в сотовом телефоне задержанного, обнаружены и изъяты еще 9 свертков с наркотическим средством¹.

Как показывает практика, телефонные устройства и иное техническое оборудование, принадлежащее лицам, имеющих причастность к совершенному или готовящемуся преступлению, имеют защиту от доступа посторонних лиц. Для этого используются пароль либо биометрические данные. Данное обстоятельство не позволяет следователю, дознавателю, а также оперативным сотрудникам осуществить мероприятия, направленные на раскрытие и расследование преступления, в максимально кратчайшие сроки. Осуществить осмотр предметов – электронных устройств на месте преступления не представляется возможным ввиду отсутствия соответствующего оборудования и специалистов. Поэтому, в целях более эффективной организации и осуществления раскрытия и расследования преступлений, предлагается:

- формировать дежурные следственно-оперативные группы, осуществляющие выезд на место происшествия, специалистами в области высоких технологий, обладающими умениями и навыками, позволяющими осуществить неотложный осмотр телефонного и иного технического оборудования, с помощью которого, возможно, было совершено преступное деяние, либо в телефонном устройстве могут содержаться сведения, имеющие отношение к расследуемому преступлению.

То есть, в случае задержания лица, совершившего преступление и обнаружения технического устройства, в дежурную часть должно поступить соответствующее сообщение с обязательным указанием на наличие технического устройства, неотложный осмотр которого необходимо произвести.

Исследования, проведенные в рамках настоящей главы, позволяют сделать следующие выводы.

¹ Приговор Таганрогского городского суда Ростовской области от 27.02.2024 по делу № 1-162/2024 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/81212788/extended> (дата обращения: 28.02.2024).

При расследовании преступлений в сфере компьютерной информации распространенным следственным действиям относятся: осмотр места происшествия, допрос всех участников – подозреваемого, потерпевшего, свидетелей; назначение экспертиз (компьютерной, дактилоскопической, портретной и т.д.), обыск и выемка.

Процесс расследования мошенничества, совершенного с использованием информационных технологий, проводятся такие следственные действия, как допрос) лица в качестве потерпевшего, в ходе которого устанавливаются обстоятельства совершенного преступления (время, место, способы обмана, способы оплаты, размер причиненного вреда и т.д.); осмотр сотового телефона, иного технического оборудования, с помощью которого велась переписка с преступником, осуществлен перевод денежных средств, а также обыск и выемка.

В ходе расследования преступлений, связанных с незаконным оборотом наркотиков, проводятся такие следственные действия, как осмотр места происшествия, в ходе которого осуществляется изъятие наркотических средств из тайниковых, осмотр телефона с разрешения фигуранта в целях отыскания фотоизображения с тайниковыми закладками для их дальнейшего изъятия СОГ. После возбуждения уголовного дела проводятся допросы подозреваемого, свидетелей (сотрудников полиции, принимавших участие в задержании, незаинтересованных лиц, участвовавших при личном досмотре, осмотре места происшествия), а также обыск.

Расследование преступлений экстремисткой направленности, местом совершения которых является цифровое пространство, включает в себя проведение таких следственных действий, как: осмотр интернет-ресурсов, на котором были размещены материалы, возможно относящиеся к категории экстремистских; назначение судебной лингвистической экспертизы экстремистских материалов. Распространенными также являются мероприятия, связанные с истребование сведений из службы безопасности или администрации интернет-ресурса на предмет получения информации о пользователе, его регистрационных данных, IP-адресе, с которого им осуществляется доступ к

ресурсу и был размещен тот или иной запрещенный материал, истребование сведений у интернет-провайдера и оператора связи о конкретном абоненте, приобщить копию договора на оказание услуг связи и т.д. Расследование преступлений террористической направленности, к примеру, публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма, совершаемых с использованием цифровых технологий, имеет сходство с процедурой расследования экстремизма.

По делам о компьютерных преступлениях, преступлениях, совершаемых с использованием информационных технологий, распространенным является производство неотложного обыска, проводимого без предварительного получения разрешения суда.

ЗАКЛЮЧЕНИЕ

Исследования, проведенные в рамках настоящей дипломной работы, позволяют сделать следующие выводы о производстве следственных действий в случаях нетерпящих отлагательства по уголовным делам о преступлениях, совершенных в сфере цифровых технологий.

В первой главе дана характеристика преступлений в сфере цифровых технологий. Путем анализа структуры и содержания действующего уголовного законодательства, а также научных статей, публикаций, посвященных рассматриваемому вопросу, установлено, что к цифровым преступлениям относятся следующие уголовно-наказуемые деяния:

- преступления, посягающие на цифровые технологии – цифровые платформы (цифровые устройства (компьютеры, смартфоны, планшеты), программное обеспечение, интернет, социальные сети и другие цифровые платформы);

- преступления, совершаемые с использованием цифровых технологий.

Первая группа уголовно-наказуемых деяний связана с неправомерным доступом к компьютерной информации, созданием, использованием и распространением вредоносных программ, нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации, нарушением правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования. То есть, это преступления, закрепленные в Главе 28 УК РФ.

Вторую группу преступлений образуют деяния, объективная сторона которых реализуется путем использования цифровых технологий:

- преступления, направленные против чести и достоинства личности, в первую очередь, клевета;
- преступления, посягающие на отношения собственности, в частности, мошенничества и его отдельные виды;
- преступления, направленные против общественной безопасности (террористического характера, в сфере незаконного оборота оружия и боеприпасов);
- преступления против здоровья населения, преимущественно связанные с незаконным оборотом наркотических средств и психотропных веществ;
- преступления против основ конституционного строя и безопасности государства: публичные призывы к осуществлению экстремистской деятельности; возбуждение ненависти либо вражды, а равно унижение человеческого достоинства.

Состав данных преступлений, как правило, содержит такой квалифицирующий признак, как «использование электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет». При анализе материалов судебно-следственной практики выявлено, что цифровые технологии используются для поиска соучастников, орудий преступления. Так, резонансным стало раскрытие первого убийства, заканного в сети «Даркнет».

Вторая глава посвящена исследованию общих положений уголовно-процессуального законодательства о производстве следственных действий в случаях, не терпящих отлагательства. В рамках второй главы определены сущность и содержание понятия «случаи, не терпящие отлагательства». В ходе анализа уголовно-процессуальных норм, а также научных статей, публикаций, посвященных рассматриваемой теме, установлено, что случаи, не терпящие отлагательства — это конкретные следственные ситуации, требующие немедленного, незамедлительного производства следственного действия в целях своевременного обнаружения и изъятия доказательств по делу, пресечения противоправной деятельности. Данная категория является оценочной, поэтому

следователь, дознаватель, орган дознания самостоятельно дают оценку возникшей обстановке и принимают решение о том, относятся ли сложившиеся условия к ситуациям, не терпящим отлагательства либо нет. В то же время в Постановлении Пленума Верховного Суда РФ, а также в некоторых ведомственных нормативно-правовых актах, в качестве случаев, не терпящих отлагательств, определены ситуации, когда:

- необходимо реализовать меры по предотвращению или пресечению преступления;
- промедление с производством следственного действия позволит подозреваемому скрыться;
- возникла реальная угроза уничтожения или сокрытия предметов, или орудий преступления;
- имеются достаточные основания полагать, что лицо, находящееся в помещении или ином месте, в котором производится какое-либо следственное действие, скрывает при себе предметы или документы, могущие иметь значение для уголовного дела.

В процессе исследования также установлено, что помимо «производства следственных действий в случаях, не терпящих отлагательства», в действующем уголовно-процессуальном законодательстве содержится схожая по смыслу и содержанию категория - неотложные следственные действия – действия, проводимые следователем, дознавателем, органом дознания в целях обнаружения и фиксации следов преступления, а также доказательств, требующих незамедлительного закрепления, изъятия и исследования. Далее сделан вывод о том, что вышеуказанные категории могут быть рассмотрены как синонимы. Данный вывод мотивирован тем, что ходе прохождения преддипломной (производственной) практики установлено, что действующие следователи, дознавателем, а также оперативные работники в своей служебной деятельности оперируют понятиями «неотложный обыск», «неотложный осмотр», понимая под этим проведение соответствующих мероприятий в целях обнаружения и изъятия предметов, документов, имеющих значение дела, когда

существующая следственная ситуация не терпит отлагательства. То есть, практические работники не видят существенную разницу между указанными уголовно-процессуальными категориями.

В связи с вышеизложенным, осуществлен анализ положений уголовно-процессуального законодательства, регламентирующих вопросы производства следственных действий случаях, не терпящих отлагательства УПК РФ, а также производства неотложных следственных действий.

Так, действующий уголовно-процессуальный закон не допускает производство следственных действий в ночное время, за исключением случаев, не терпящих отлагательства. Проведение следственных действий, которые носят поисковый характер и связаны с изъятием предметов, в первую очередь, следственного осмотра, обыска, выемки в ночное время является вполне обоснованным решением. Далее возник вопрос: целесообразно ли распространять норму, закрепленную в части 3 статьи 164 УПК РФ на группу следственных действий, которые, допустим, не носят поисковый характер, а связаны с получением показаний – допрос, очная ставка, проверка показаний на месте? Дело в том, что в ночное время суток сознание человека характеризуется снижением процессов жизнедеятельности, что в значительных случаях не способствует получению полных и правдивых показаний. Следует учесть, что допрос не является единственным способом получения показаний. Информация, имеющая существенное значение для хода и направления расследования может быть получена путем производства оперативно-розыскного мероприятия «Опрос», который носит более упрощенный характер и не имеет процессуальные рамки. В связи с вышеизложенным предлагается сформулировать ч.3 ст. 164 УПК РФ следующим образом:

- В ночное время недопустимо производство допроса, очной ставки, проверки показаний на месте, предъявления для опознания. Иные следственные действия могут быть проведены в случаях, не терпящих отлагательства.

Помимо статьи 164 УПК РФ, в статье 179 законодатель допускает производство неотложного освидетельствования. В отличие от предыдущей,

нормы, закрепленные в статье 179 УПК РФ, не носят проблемный характер и не требуют совершенствования.

В статье 165 закреплены нормы, определяющие судебный порядок получения разрешения на производство следственных действий, ограничивающих конституционные права граждан. При наличии исключительных случаев, не терпящих отлагательства, производство указанной категории следственных действий возможно без предварительного получения судебной санкции.

Субъектами производства неотложных следственных действий выступают следователь, дознаватель, орган дознания, а также капитаны морских и речных судов, руководители геологоразведочных партий и зимовок, глав дипломатических представительств и иные лица, указанные в статье 40 УПК РФ. Орган дознания, проводившие неотложные следственные действия, не позднее 10 суток со дня возбуждения уголовного дела направляет уголовное дело руководителю следственного органа в соответствии с пунктом 3 статьи 149 УПК РФ.

В рамках третьей главы определена процедура расследования уголовных дел о преступлениях, совершенных в сфере цифровых технологий, а также рассмотрены вопросы производства отдельных следственных действий в случаях, не терпящих отлагательства.

При анализе материалов судебно-следственной практики установлено, что мошенничество и преступления в сфере компьютерной информации нередко образуют совокупность. При расследовании данных преступлений неотложный характер чаще всего носит обыск в жилище, который проводится без предварительного получения судебного разрешения. Как показывает практика, в ходе которого осуществляется обнаружение и изъятие орудий и средств совершения преступления – технического оборудования (компьютеры, ноутбуки, сотовые телефоны), а также средств связи, денежных средств, добытых преступным путем, банковских карт.

Производство неотложного обыска имеет место при расследовании преступлений, связанных с незаконным оборотом наркотиков, совершаемых с использованием информационно-телекоммуникационных технологий. В ходе обыска происходит обнаружение и изъятие предмета данной категории уголовно-наказуемых предметов – наркотических средств и психотропных веществ.

Как показывает практика, телефонные устройства и иное техническое оборудование, принадлежащее лицам, имеющих причастность к совершенному или готовящемуся преступлению, имеют защиту от доступа посторонних лиц. Для этого используются пароль либо биометрические данные. Так, по делам о наркотиках лицо может оборудовать тайниковые закладки до задержания и отправить фотографии с местоположением наркотиков оператору до производства задержания. Изъятие наркотиков возможно лишь в том случае, если задержанный лично откроет мобильное устройство и покажет фотографии с закладками. В противном случае, обнаружение и изъятие запрещенных веществ не представляется возможным. Таким образом, данное обстоятельство не позволяет следователю, дознавателю, а также оперативным сотрудникам осуществить мероприятия, направленные на раскрытие и расследование преступления, в максимально кратчайшие сроки. Осуществить осмотр предметов – электронных устройств на месте преступления не представляется возможным ввиду отсутствия соответствующего оборудования и специалистов. В связи с вышеизложенным, нами предложено:

- формировать дежурные следственно-оперативные группы, осуществляющие выезд на место происшествия, специалистами в области высоких технологий, обладающими умениями и навыками, позволяющими осуществить неотложный осмотр телефонного и иного технического оборудования, с помощью которого, возможно, было совершено преступное деяние, либо в телефонном устройстве могут содержаться сведения, имеющие отношение к расследуемому преступлению.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации от 12.12.1993 г.: Принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Официальный интернет-портал правовой информации www.pravo.gov.ru, 04.07.2020. № 0001202007040001 (дата обращения: 11.10.2023).
2. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ // Российская газета. – 2001. – № 249.
3. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г N 187 ФЗ - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 17.10.2023).

II. Монографии, учебники, учебные пособия:

4. Уголовный процесс: учебник для вузов / Б. Я. Гаврилов [и др.]; под редакцией Б. Я. Гаврилова. — 9-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 572 с.
5. Гриненко, А. В. Уголовный процесс: учебник и практикум для вузов / А. В. Гриненко. — 9-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 361 с.
6. Досудебное производство в уголовном процессе: учебное пособие для вузов / Б. Б. Булатов [и др.]; под редакцией Б. Б. Булатова, А. М. Баранова. — 8-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 214 с.
7. Луковников, Г. Д. Следственные действия и оперативно-розыскные мероприятия: учебное пособие для вузов / Г. Д. Луковников. — 2-е изд. — Москва: Издательство Юрайт, 2024. — 290 с.

8. Манова, Н. С. Уголовный процесс: учебное пособие для вузов / Н. С. Манова, Ю. В. Францифоров, Н. О. Овчинникова. — 15-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 276 с.

9. Уголовно-процессуальное право Российской Федерации. Общая часть: учебник для вузов / Г. М. Резник [и др.]; под общей редакцией Г. М. Резника. — 4-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 452 с.

III. Статьи, научные публикации:

10. Алексеева Е.С. Категория «Случаи, не терпящие отлагательства» в уголовно-процессуальном законодательстве и правоприменительной практике. Вестник Санкт-Петербургского университета МВД России. — 2019. — № (4 (84)). — С. 124-130.

11. Глазунова И.В., Кудрявцев П.А. Освидетельствование как способ обнаружения и фиксации следов при расследовании преступлений. Вестник Российской таможенной академии. — 2017. — № 2. — С. 64-71.

12. Гриненко А. В. Уголовный процесс: учебник и практикум для среднего профессионального образования / А. В. Гриненко. — 9-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. С. 171.

13. Назаров А.Д., Баянов А.И., Мажинский В.А.. О целесообразности проведения следственных действий, предполагающих получение показаний, в ночное время при наличии случаев, не терпящих отлагательства. Вестник Сибирского юридического института МВД России. — 2021. — № (4 (45)), С. 190-196.

14. Лустач, К. Д. Неотложные следственные действия: понятие и проблемы правового регулирования / К. Д. Лустач // Альманах молодого исследователя. — 2022. — № 12. — С. 99-103.

15. Манова Н.С. «Ситуация, не терпящая отлагательства» как оценочная категория в законодательстве и практике уголовного судопроизводства. Legal Concept, — 2019. — №18 (2), С. 42-48.

16. Огородник А. В. История возникновения кибертерроризма: от киберпреступности до кибертерроризма / А. В. Огородник // Донецкие чтения 2021: образование, наука, инновации, культура и вызовы современности: Материалы VI Международной научной конференции, Донецк, 26–28 октября 2021 года / Под общей редакцией С.В. Беспаловой. – Донецк: Донецкий национальный университет, 2021. С. 147.

17. Поляков И.В. Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. – № 4. – 2020. – С. 21-25.

18. Харламова А.А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации. Вестник Уральского юридического института МВД России. – № 2. – 2020. – С. 165.

19. Шурухнов Н. Г. Качество неотложных следственных действий как необходимое условие эффективности расследования: к проблеме использования информационных технологий / Н. Г. Шурухнов // Российский следователь. – 2020. – № 8. – С. 18-22.

IV. Эмпирические материалы:

20. О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ): Постановление Пленума Верховного Суда РФ от 01.06.2017 № 19 - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 25.12.2023)

21. Постановление Нижнекамского городского суда (Республика Татарстан) от 28 мая 2020 года по делу № 1-245/2020. - [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/vDG8KdwkPKbO/> (дата обращения: 30.01.2024).

22. Постановление Рыбинского городского суда Ярославской области от 17.03.2023 по делу № 1-138/2023 [Электронный ресурс] // URL: <https://судебныерешения.рф/74493375/extended> (дата обращения: 04.11.2023).

23. Приговор Чухломского районного суда Костромской области 02.05.2023 года по делу № 1-19/2023[Электронный ресурс] // URL: <https://судебныерешения.рф/74195703/extended> (дата обращения: 25.10.2023).

24. Приговор Великолукского городского суда (Псковская область) от 21 января 2020 года по делу № 1-18/2020 [Электронный ресурс]. URL:<https://sudact.ru/regular/doc/ReZKsD98lIx/> (дата обращения: 30.10.2023).

25. Приговор Ленинского районного суда г. Кирова (Кировская область) № 1-255/2020 от 17 апреля 2020 г. по делу № 1-255/2020 33. - [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/QE4e5xM6l66T/> (дата обращения: 08.01.2024).

26. Приговор Московского районного суда г. Калининград от 06.10.2023 по делу № 1-237/2023 33. - [Электронный ресурс]. – URL: <https://судебныерешения.рф/77116661/extended> (дата обращения: 26.01.2023).

27. Приговор Октябрьского районного суда г. Ставрополя от 02.11.2023 по делу № 1-354/2023 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/78771438/extended> (дата обращения: 07.02.2024).

28. Приговор Первомайского районного суда г. Краснодара от 19.07.2018 по делу № 1-50/2018 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/35324463/extended> (дата обращения: 27.02.2024).

29. Приговор Советского районного суда г. Орел от 28.11.2022 по делу № 1-242/2022 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/72706234/extended> (дата обращения 09.11.2023).

30. Приговор Воскресенского городского суда Московской области от 26.05.2022 по делу № 1-143/2022 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/66972674/extended> (дата обращения: 16.11.2023).

31. Приговор Кунгурского городского суда Пермского края от 30.08.2023 по делу № 1-420/2023 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/78050899/extended> (дата обращения: 21.11.2023).

32. Приговор Ломоносовского районного суда г. Архангельск от 19.09.2023 по делу № 1-509/2023 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/77868426/extended> (дата обращения: 27.11.2023).

33. Приговор Приволжского районного суда г. Казани (Республика Татарстан) от 24 июля 2019 г. по делу № 1-317/2019 [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/Py1ROQEJXQWq/> (дата обращения: 28.02.2024).

34. Приговор Таганрогского городского суда Ростовской области от 27.02.2024 по делу № 1-162/2024 - [Электронный ресурс]. – URL: <https://судебныерешения.рф/81212788/extended> (дата обращения: 28.02.2024).

V. Справочная литература:

35. «Татарский маньяк» и «Казанский Брейвик» за фейки не ответят. [Электронный ресурс] // Вечерняя Казань | Дзен URL: https://dzen.ru/a/ZZ44sicKAQiquXp_ (дата обращения 09.11.2023).

36. Цифровые технологии (в праве) [Электронный ресурс] // Большая российская энциклопедия URL: <https://bigenc.ru/c/tsifrovye-tekhnologii-v-prave-a80897> (дата обращения: 05.10.2023).

37. Задержан организатор заказных убийств через даркнет [Электронный ресурс] // Российская газета URL: <https://rg.ru/2021/09/09/reg-pfo/zaderzhan-organizator-zakaznyh-ubijstv-cherez-darknet.html> (дата обращения 08.10.2023).