Академия управления МВД России

Ю. В. Гаврилин, Н. Э. Мартыненко, И. С. Бедеров

ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ЗАВЕДОМО ЛОЖНЫХ СООБЩЕНИЙ ОБ АКТАХ ТЕРРОРИЗМА

Учебное пособие

Москва
2023

УДК 343.9
ББК 67.408
Г12

Одобрено редакционно-издательским советом Академии управления МВД России

Рецензенты: *Мешалкин С. Н.*, доктор юридических наук, доцент (ВНИИ МВД России); *Тишутина И. В.*, доктор юридических наук, доцент (Московский университет МВД России имени В. Я. Кикотя).

Гаврилин, Юрий Викторович.

Г12 Организация расследования заведомо ложных сообщений об актах терроризма : учебное пособие / Ю. В. Гаврилин, Н. Э. Мартыненко, И. С. Бедеров. – Москва : Академия управления МВД России, 2023. – 76 с.

ISBN 978-5-907530-85-0

В учебном пособии рассматриваются теоретические и практические вопросы, связанные с организацией расследования заведомо ложных сообщений об актах терроризма.

Учебное издание предназначено для адъюнктов (аспирантов), проходящих обучение в адъюнктуре (аспирантуре) по направлению подготовки 5.1.4 «Уголовно-правовые науки», и слушателей образовательных организаций МВД России, а также может представлять интерес для сотрудников предварительного следствия и дознания.

УДК 343.9
ББК 67.408

ISBN 978-5-907530-85-0

Авторский коллектив

Гаврилин Юрий Викторович, д-р юрид. наук, проф. – введение, гл. 2, 3, 4 (совместно с И. С. Бедеровым), заключение;

Мартыненко Наталия Эдуардовна, д-р юрид. наук, проф. – гл. 1;

Бедеров Игорь Сергеевич – гл. 4 (совместно с Ю. В. Гаврилиным)

Оглавление

Введение 5

Глава 1. Уголовная ответственность за заведомо ложное сообщение об акте терроризма. 7

Глава 2. Особенности механизма совершения заведомо ложных сообщений об актах терроризма 32

Глава 3. Алгоритм действий следователя и сотрудников оперативных подразделений МВД России на этапе проверки и первоначальном этапе расследования заведомо ложных сообщений об актах терроризма 42

Глава 4. Методы и средства получения и анализа информации из открытых источников, используемые для установления личности отправителей заведомо ложных сообщений об актах терроризма 48

Заключение 71

Список рекомендованной литературы 72

Введение

Заведомо ложное сообщение об акте терроризма – преступление с давней историей. Впервые массовый характер данное явление начало приобретать в начале 90-х гг. прошлого века. Совершалось оно, как правило, из хулиганских побуждений, преимущественно подростками, с использованием стационарной телефонной связи и уличных таксофонов. Однако достаточно быстро органы внутренних дел Российской Федерации выработали методические подходы к их раскрытию и расследованию, чему способствовало развитие технологий фиксации речевой информации в дежурных частях и возможностей фоноскопической экспертизы. Некоторое время количество данных преступлений находилось на невысоком уровне.

Вторая волна подобных лжеминирований прокатилась по стране на фоне роста террористической угрозы, связанной с деятельностью международных террористических организаций в Северо-Кавказском регионе Российской Федерации, а также серии криминальных взрывов жилых домов в Буйнакске, Москве, Волгодонске. При этом механизм их совершения и методика расследования существенных изменений не претерпели.

Ситуация радикально изменилась с развитием современных информационно-телекоммуникационных технологий: электронной почты, интернет-телефонии, сервисов мгновенного обмена сообщениями, социальных сетей и др. Использование подобных средств коммуникации совместно со средствами анонимизации, обеспечивающими сокрытие или подмену основных цифровых следов, существенным образом преобразовало механизм совершения заведомо ложного сообщения об акте терроризма. Объектами угрозы взрыва по-прежнему остались учебные заведения, вокзалы, гостиницы, магазины, различные учреждения, организации и другие общественные места. Однако изменились технологии передачи сообщения, а также мотивы совершения подобных деяний. На смену хулиганским мотивам все чаще приходят политические требования, актуальные для текущего исторического периода.

На проверку таких сообщений затрачиваются значительные материальные средства, задействуются многочисленные человеческие ресурсы. Кроме того, парализуется работа транспорта, предприятий и учреждений, создается нервозная обстановка, в обществе возникает атмосфера страха и т. д.

В связи с тем, что данные сообщения в большинстве случаев направляются посредством электронной почты, IP-адрес которой зарегистрирован за пределами Российской Федерации, установле-

ние обстоятельств, подлежащих доказыванию, а также лица, направившего по электронной почте сообщение о заведомо ложном акте терроризма, при расследовании данной категории преступлений вызывает некоторые сложности в определении объема причиненного ущерба объекту угрозы в результате ложного сообщения, материального ущерба, причиненного правоохранительным органам и иным службам оперативного реагирования в результате проведения мероприятий по проверке поступившего сообщения.

Кроме того, ложные сообщения об актах терроризма сопровождаются требованиями о перечислении на электронные кошельки денежных средств, поэтому возникают сложности отграничения указанных преступлений от смежных составов либо необходимость дополнительной квалификации действий подозреваемых (обвиняемых) по иным составам.

Повышенный общественный резонанс и значительный ущерб, причиняемый заведомо ложными сообщениями об актах терроризма, определяют актуальность научных исследований по данному направлению. С учетом изложенного и отсутствием актуальных методических подходов назрела необходимость разработки специального методического обеспечения расследования заведомо ложных сообщений об актах терроризма, рекомендаций по правильной квалификации преступлений по ст. 207 Уголовного кодекса Российской Федерации, отграничению от смежных составов, в том числе ст. 163 Уголовного кодекса Российской Федерации.

В основу учебного пособия легли результаты научно-исследовательской работы, проведенной членами авторского коллектива в 2022 г. по заказу Следственного департамента МВД России.

Глава 1. Уголовная ответственность за заведомо ложное сообщение об акте терроризма

Социальная обусловленность уголовной ответственности за заведомо ложное сообщение об акте терроризма

Проблеме социальной обусловленности уголовно-правового запрета в науке уголовного права уделялось достаточно много внимания. Социальную обусловленность, как правило, связывают с причинением деянием существенного вреда общественному отношению, антиобщественной ориентацией лица, распространенностью деяния и его повышенной угрозой для общества, неэффективностью других некриминальных мер, способностью общественного сознания воспринять это деяние как преступление[1].

Точкой отсчета для разработки любой новой уголовно-правовой нормы выступает появление новых видов общественно опасного поведения, представляющего собой угрозу для нормального порядка функционирования общества.

Уголовная ответственность за заведомо ложное сообщение об акте терроризма была установлена в 1994 г. в Уголовном кодексе Российской Советской Федеративной Социалистической Республики (далее – УК РСФСР)[2].

В первоначальной редакции ст. 213.4 УК РСФСР предусматривала ответственность за заведомо ложное сообщение о готовящемся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба, а равно наступления иных тяжких последствий. Санкция статьи предусматривала наказания в виде лишения свободы на срок до трех лет или штраф до тридцати минимальных размеров оплаты труда.

Уголовный кодекс Российской Федерации[3] (далее – УК РФ) 1996 г. фактически сохранил редакцию, которая была предусмотрена УК РСФСР, отнеся заведомо ложное сообщение об акте

---

[1] *Кригер Г. А., Кузнецова Н. Ф.* Проблемы социальной обусловленности уголовного закона. М., 1977. С. 34.

[2] О внесении изменений и дополнений в Уголовный кодекс РСФСР и Уголовно-процессуальный кодекс РСФСР : Федер. закон № 10-ФЗ : утратил силу // Собр. законодательства Рос. Федерации. 1994. № 10. Ст. 1109.

[3] Уголовный кодекс Российской Федерации : Федер. закон № 63-ФЗ : принят Гос. Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. : в ред. от 13 июня 1996 г.

терроризма (ст. 207 УК РФ) к категории преступлений средней тяжести, что давало возможность при наличии к тому обстоятельств прекратить уголовное дело, например, за деятельным раскаянием (ст. 75 УК РФ).

За время действия рассматриваемой статьи в нее были внесены изменения и дополнения, направленные на ужесточение уголовной ответственности в связи с ростом количества совершаемых преступлений.

В 2014 г. введен новый квалифицированный состав преступлений заведомо ложного сообщения об акте терроризма. Новый состав преступления (ч. 2 ст. 207 УК РФ) предусматривает ответственность за заведомо ложное сообщение об акте терроризма, повлекшее за собой причинение крупного ущерба (на сумму свыше 1 млн руб.) либо наступление иных тяжких последствий. За данное преступление теперь предусмотрен штраф в размере до 1 млн руб. либо лишение свободы на срок до 5 лет[1].

Необходимость внесения данного изменения разработчиками законопроекта обосновывалась увеличением в течение последних пяти лет (по данным статистики – в среднем на 15 % в год) количества преступлений, предусмотренных ст. 207 УК РФ, и большим материальным ущербом по факту проверки информации о ложном сообщении об акте терроризма. Однако данные изменения уголовного закона не дали ожидаемого эффекта и количество преступлений, предусмотренных ст. 207 УК РФ, продолжало расти (таблица 1).

и в ред. от 4 авг. 2023 г. // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 22.08.2023). Режим доступа: для зарегистрир. пользователей.

[1] О внесении изменений в статью 207 Уголовного кодекса Российской Федерации и статьи 150 и 151 Уголовно-процессуального кодекса Российской Федерации : Федер. закон № 98-ФЗ : принят Гос. Думой 15 апр. 2014 г. : одобрен Советом Федерации 29 апр. 2014 г. // Собр. законодательства Рос. Федерации. 2014. № 19. Ст. 2303.

Таблица 1

**Количество преступлений,
зарегистрированных по ст. 207 УК РФ
(по данным ГИАЦ МВД России (форма 491 раздел 10))**

Год	Количество преступлений, зарегистрированных в отчетном периоде	Количество преступлений, уголовные дела о которых приостановлены по ч. 1 ст. 208 Уголовно-процессуального кодекса Российской Федерации		
		п. 1	п. 2	п. 3
2011	1 878	1 118	0	0
2012	1 252	529	0	0
2013	1 250	396	0	0
2014	1 355	432	11	9
2015	1 634	627	17	24
2016	1 466	513	14	9
2017	3 027	1 481	17	15
2018	1 530	1 144	54	10
2019	2 456	1 289	29	5
2020	2 404	1 698	19	10
2021	3 018	1 806	20	2
2022	23 247	19 400	79	1

Наиболее часто предварительное следствие приостанавливается из-за того, что лицо, подлежащее привлечению в качестве обвиняемого по ст. 207 УК РФ, не установлено. В 2011 г. по п. 1 ч. 1 ст. 208 Уголовно-процессуального кодекса Российской Федерации[1] (далее – УПК РФ) было приостановлено 59,5 % от зарегистрированных преступлений, предусмотренных ст. 207 УК РФ, 2012 г. – 42,2 %, 2013 г. – 31,7 %, 2014 г. – 31,9 %, 2015 г. – 38,4 %, 2016 г. – 35 %, 2017 г. – 48,9 %, 2018 г. – 74,7 %, 2019 г. – 52,5 %, 2020 г. – 70,6 %, 2021 г. – 60 %, 2022 г. – 83,7 %.

Статистические данные о количестве приостановленных уголовных дел позволяют предположить, что проблема противодей-

[1] Уголовно-процессуальный кодекс Российской Федерации : Федер. закон № 174-ФЗ : принят Гос. Думой 22 нояб. 2001 г. : одобрен Советом Федерации 5 дек. 2001 г. : в ред. от 4 авг. 2023 г. // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 21.08.2023). Режим доступа: для зарегистрир. пользователей.

ствия противоправным деяниям, связанным с заведомо ложным сообщением об акте терроризма, кроется не в законодательной конструкции ст. 207 УК РФ, а в том, что правоприменительные органы не всегда могут (в силу различных причин) выявить лиц, которые сообщают заведомо ложную информацию об акте терроризма.

В 2017 г. редакция ст. 207 УК РФ подверглась изменению Федеральным законом от 31 декабря 2017 г. № 501-ФЗ «О внесении изменений в статьи 205 и 207 Уголовного кодекса Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации»[1]. В пояснительной записке к законопроекту отмечалось, что всего по России с 11 по 25 сентября 2017 г. было эвакуировано порядка 450 тыс. человек, зафиксировано около 1 тыс. анонимных звонков о «минировании». По данным МЧС России, 1 млрд руб. является минимальной границей ущерба от ложных звонков о минировании[2].

Кроме того, вышеназванным Федеральным законом была существенно изменена диспозиция ч. 1 ст. 207 УК РФ. Теперь для привлечения к уголовной ответственности необходимо, чтобы деяния, перечисленные в диспозиции, были совершены из хулиганских побуждений. Таким образом, мотив совершения преступления из факультативного стал обязательным признаком субъективной стороны состава преступления. При этом наличие других мотивов (ненависть, корысть и т. д.) не позволяет отнести содеянное к заведомо ложному сообщению об акте терроризма.

Помимо мотива, изменения коснулись диспозиции ч. 2 ст. 207 УК РФ. Кроме того, статья была дополнена двумя новыми квалифицирующими признаками (ч. 3 и ч. 4). В таблице 2 представлены изменения и дополнения, внесенные в ст. 207 УК РФ.

---

[1] О внесении изменений в статьи 205 и 207 Уголовного кодекса Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации : Федер. закон № 501-ФЗ : принят Гос. Думой 20 дек. 2017 г. : одобрен Советом Федерации 26 дек. 2017 г. // Собр. законодательства Рос. Федерации. 2018. № 1 (ч. 1). Ст. 85.

[2] Пояснительная записка к проекту Федерального закона № 322801-7 «О внесении изменений в статью 207 Уголовного кодекса Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации» (в части усиления ответственности за заведомо ложное сообщение об акте терроризма) // СОЗД ГАС «Законотворчество» : сайт. URL: https://sozd.duma.gov.ru/bill/322801-7?sortEventsByNum=num_up&sortEventsByDate=datend_down (дата обращения: 15.05.2023).

Таблица 2

Изменения и дополнения, внесенные в ст. 207 УК РФ

Ст. 207. Заведомо ложное сообщение об акте терроризма в УК РФ (в ред. от 13 июня 1996 г.)	**Федеральный закон от 5 мая 2014 г. № 98-ФЗ «О внесении изменений в статью 207 Уголовного кодекса Российской Федерации и статьи 150 и 151 Уголовно-процессуального кодекса Российской Федерации»**	**Федеральный закон от 31 декабря 2017 г. № 501-ФЗ «О внесении изменений в статьи 205 и 207 Уголовного кодекса Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации»**
Ст. 207. Заведомо ложное сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до трех лет	1) в абзаце первом слова «Заведомо ложное» заменить словами «1. Заведомо ложное»; 2) дополнить частью второй следующего содержания: «2. То же деяние, повлекшее причинение крупного ущерба либо наступление иных тяжких последствий, – наказывается штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от восемнадцати месяцев до трех лет либо лишением свободы на срок до пяти лет»; 3) дополнить примечанием следующего содержания: «Примечание. Крупным ущербом в настоящей статье признается ущерб, сумма которого превышает один миллион рублей»	Ст. 207. Заведомо ложное сообщение об акте терроризма 1. Заведомо ложное сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, совершенное из хулиганских побуждений, – наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до восемнадцати месяцев, либо ограничением свободы на срок до трех лет, либо принудительными работами на срок от двух до трех лет. 2. Деяние, предусмотренное частью первой настоящей статьи, совершенное в отношении объектов социальной инфраструктуры либо повлекшее причинение крупного ущерба, – наказывается штрафом в размере от пятисот тысяч до семисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет либо лишением свободы на срок от трех до пяти лет. 3. Заведомо ложное сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий в целях дестабилизации деятельности органов власти, – наказывается штрафом в размере от семисот тысяч до одного

		миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок от шести до восьми лет. 4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, повлекшие по неосторожности смерть человека или иные тяжкие последствия, – наказываются штрафом в размере от одного миллиона пятисот тысяч до двух миллионов рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет либо лишением свободы на срок от восьми до десяти лет. Примечания. 1. Крупным ущербом в настоящей статье признается ущерб, сумма которого превышает один миллион рублей. 2. Под объектами социальной инфраструктуры в настоящей статье понимаются организации систем здравоохранения, образования, дошкольного воспитания, предприятия и организации, связанные с отдыхом и досугом, сферы услуг, пассажирского транспорта, спортивно-оздоровительные учреждения, система учреждений, оказывающих услуги правового и финансово-кредитного характера, а также иные объекты социальной инфраструктуры

Таким образом, социальная обусловленность включения в УК РФ статьи, предусматривающей ответственность за заведомо ложное сообщение об акте терроризма, и внесение в нее изменений и дополнений в первую очередь связаны с изменением характера и повышением степени общественной опасности данного преступления, что проявляется в увеличении количества ложных сообщений об актах терроризма, изменении способа их совершения.

Объективные и субъективные признаки заведомо ложного сообщения об акте терроризма. Уголовная ответственность за заведомо ложное сообщение об акте терроризма предусмотрена ст. 207 УК РФ, расположенной в гл. 24 «Преступления против

общественной безопасности» раздела IX «Преступления против общественной безопасности и порядка».

Действующая ст. 207 УК РФ включает в себя четыре части. Ч. 1 относится к категории небольшой тяжести, ч. 2 – средней тяжести, ч. 3 и 4 – к категории тяжкого преступления.

Название ст. 207 УК РФ включает словосочетание «акт терроризма», тогда как ст. 205 УК РФ носит название «Террористический акт». Являются ли синонимами эти термины? Ответ на этот вопрос важен, потому что существующая терминологическая неразбериха осложняет работу правоприменительной практики при отграничении ст. 205 от ст. 207 УК РФ. Что касается судебного толкования, то в постановлении Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1[1] содержится только толкование террористического акта.

В научной литературе эти термины нередко предлагают считать синонимами. Однако некоторые специалисты утверждают, что между этими терминами есть различие. Так, например, акт терроризма может выражаться не только в насильственных действиях, повлекших реальные последствия, но и в угрозе совершения таких действий и даже бездействия, тогда как содержание понятия «террористический акт» охватывает лишь реально совершившиеся действия[2].

Для унификации положений, закрепленных в ст. 205 и 207 УК РФ, целесообразно использовать одинаковые термины. Этим термином должен быть террористический акт, так как именно его понятие содержится в Федеральном законе от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»[3].

Объект преступления. В российском уголовном праве принято классифицировать объекты преступления по двум основаниям:

– «по вертикали» – общий, родовой, видовой и непосредственный;

– «по горизонтали» (на уровне непосредственного объекта) – основной, дополнительный и факультативный.

---

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности : постановление Пленума Верховного Суда Рос. Федерации от 9 февр. 2012 г. № 1 : в ред. от 3 нояб. 2016 г. // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 15.05.2023). Режим доступа: для зарегистрир. пользователей.

[2] *Емельянов В. П.* Террористический акт и акт терроризма: понятие, соотношение и разграничение // Законность. 2002. № 7. С. 44–46.

[3] О противодействии терроризму : Федер. закон № 35-ФЗ : принят Гос. Думой 26 февр. 2006 г. : одобрен Советом Федерации 1 марта 2006 г. : в ред. от 10 июля 2023 г. // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 15.07.2023). Режим доступа: для зарегистрир. пользователей.

Классификация объекта «по вертикали».

Общий объект всех преступлений одинаков и, как правило, не выделяется.

Родовым объектом преступления, предусмотренного ст. 207 УК РФ, является общественная безопасность. Под общественной безопасностью принято понимать состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Именно такое определение безопасности содержалось в Законе Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности»[1]. Общественная безопасность как родовой объект преступления – это общественные отношения, обеспечивающие охрану безопасной жизнедеятельности граждан, общества и государства, функционирование и развитие его институтов. В изученных приговорах безопасность жизнедеятельности граждан описывается следующим образом: совершил заведомо ложное сообщение об акте терроризма для создания паники, страха, беспокойства, парализации нормальной деятельности учреждения, отвлечения сил правоохранительных органов и специальных служб, призванных оказывать помощь в экстремальных ситуациях; нарушения нормальной деятельности государственных учреждений; дезорганизации нормальной деятельности учреждений, вынужденных реагировать на сообщение.

Видовой объект. Традиционно считалось, что видовым объектом преступления, предусмотренного ст. 207 УК РФ, являются общественные отношения, обеспечивающие общественную безопасность[2]. Однако дополнение в 2017 г. диспозиции статьи указанием на совершение заведомо ложного сообщения об акте терроризма из хулиганских побуждений позволяет говорить о том, что теперь видовым объектом является не только общественная безопасность, но и общественный порядок.

Непосредственный объект ст. 207 УК РФ совпадает с видовым объектом.

Классификация объекта «по горизонтали».

Основным объектом преступления является общественная безопасность. Дополнительным – общественные отношения, охраняющие порядок управления, интересы правосудия и др.

Объективная сторона преступления. Диспозиция ч. 1 ст. 207 УК РФ сконструирована следующим образом: «Заведомо ложное сообщение

---

[1] О безопасности : Закон Рос. Федерации № 2446-1 : в ред. от 26 июня 2008 г. : утратил силу // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 15.07.2023). Режим доступа: для зарегистрир. пользователей.

[2] Уголовное право. Особенная часть : учеб. для вузов / под ред. И. Я. Козаченко, З. А. Незнамовой, Г. П. Новоселова. М., 1997. С. 377.

о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, совершенное из хулиганских побуждений».

Тем самым объективная сторона преступления включает в себя совокупность следующих действий:

1) сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий;

2) сообщение должно быть ложным, т. е. не соответствующим действительности. Этот признак является объективно-субъективным, поскольку сообщение не соответствует действительности и информатор заведомо знает об этом.

1. Сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий.

Ст. 207 УК РФ носит название «Заведомо ложное сообщение об акте терроризма», что позволяет утверждать, что ее диспозиция должна содержать признаки террористического акта, т. е. лицо должно сообщать ложную информацию об акте терроризма, понятие которого содержится в Федеральном законе от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» и в ст. 205 УК РФ (таблица 3).

Таблица 3

Понятие террористического акта, содержащееся в Федеральном законе от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» и в ст. 205 УК РФ

Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»	**Ст. 205 УК РФ**
Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в тех же целях	Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями

Подробное разъяснение признаков террористического акта дано Верховным Судом Российской Федерации[1].

Однако изменения, внесенные в ст. 207 УК РФ в 2017 г. (включение в ч. 1 и 2 указания на хулиганские побуждения), нарушили гармонизацию данной статьи с Федеральным законом от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» и со ст. 205 УК РФ. Фактически законодатель сконструировал нормы (ч. 1 и 2 ст. 207 УК РФ), не отражающие суть террористического акта. Поэтому лицо привлекается к уголовной ответственности не только за заведомо ложное сообщение об акте терроризма, но и за заведомо ложное сообщение об иных событиях, не являющихся актом терроризма. Включение в одну статью разных по содержанию деяний и, как следствие, появление разного объекта уголовно-правовой охраны требуют либо изменения названия статьи, либо исключения из нее ч. 1 и 2, так как они предусматривают ответственность за деяние, которое не является актом терроризма.

Для привлечения к уголовной ответственности необходимо, чтобы лицо сообщило о готовящихся взрыве; поджоге; иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. В науке уголовного права не имеет однозначного решения проблема квалификации заведомо ложного сообщения не об акте терроризма, а об акте диверсии, вандализма, пиратства, бандитизма, захвата заложников, и т. д. Существует точка зрения, что и заведомо ложное сообщение об иных «схожих» действиях также должно квалифицироваться по ст. 207 УК РФ, поскольку способы совершения преступления при террористическом акте и, например, диверсии, в основном совпадают[2]. Такое расширительное толкование норм уголовного закона может привести к их неверному применению. Более точным представляется буквальное толкование исходя из названия статьи – заведомо ложное сообщение об акте терроризма, т. е. сообщение только об акте терроризма. Данная норма была принята в целях противодействия терроризму (террористическому акту). Объектом уголовно-правовой охраны в данном случае является

---

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности : постановление Пленума Верховного Суда Рос. Федерации от 9 февр. 2012 г. № 1 : в ред. от 3 нояб. 2016 г. // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 15.05.2023). Режим доступа: для зарегистрир. пользователей.

[2] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Г. Н. Борзенков [и др.] ; отв. ред. В. М. Лебедев. 7-е изд., перераб. и доп. М., 2007. С. 625.

общественная безопасность. Распространение заведомо ложной информации, например о диверсии, посягает прежде всего на интересы государственной власти.

Сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий может быть устным или письменным. Однако в законе не содержится перечень адресатов, которым сообщаются ложные сведения.

В Российской Федерации существует законный порядок подачи обращений. Правила подачи обращений предусмотрены в Федеральном законе от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»[1]. Ведомственные инструкции правоохранительных органов, реализуя положения вышеназванного Федерального закона, регламентируют правила подачи заявлений[2].

Однако заведомо ложное сообщение об акте терроризма может быть адресовано не только правоохранительным органам, но и организациям, предприятиям либо учреждениям любой формы собственности, органам государственной власти или местного самоуправления, средствам массовой информации и др.

Изучение судебных приговоров показало, что они направляются на следующие телефонные номера:

– «112» – номер единой дежурно-диспетчерской службы (ЕДДС);

– правоохранительных органов (прокуратуры, ФСБ России, МВД России);

– судов;

– администрации города, района и т. д.;

– аэропорта;

– торгового центра (магазина);

---

[1] О порядке рассмотрения обращений граждан Российской Федерации : Федер. закон № 59-ФЗ : принят Гос. Думой 21 апр. 2006 г. : одобрен Советом Федерации 26 апр. 2006 г. : в ред. от 27 дек. 2018 г. // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 15.07.2023). Режим доступа: для зарегистрир. пользователей.

[2] Об утверждении Инструкции об организации рассмотрения обращений граждан Российской Федерации в органах федеральной службы безопасности : приказ ФСБ России от 30 авг. 2013 г. № 463 // Рос. газ. 2013. 4 дек.; Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях : приказ МВД России от 29 авг. 2014 г. № 736 : в ред. от 9 окт. 2019 г.

– образовательной организации;
– городской больницы;
– офиса банка.

В последние годы возрастает количество направлений электронных заведомо ложных сообщений через официальные сайты или электронную приемную организаций. Подобные действия изменяют характер и повышают степень общественной опасности преступления, так как одновременно осуществляется рассылка сообщений о совершении акта терроризма сразу нескольким адресатам (например, в 15 образовательных организаций). В связи с этим представляется целесообразным дополнить ст. 207 УК РФ новым отягчающим обстоятельством – совершением преступления с использованием информационно-телекоммуникационной системы Интернет.

Изучение материалов судебной практики показало, что электронные сообщения направляются на электронный адрес городской администрации, ГУ МЧС России, УФСБ России, финансово-кредитного колледжа, общеобразовательной школы и т. д.

Еще одним новым способом является распространение ложной информации в закрытых группах в Интернете, например в социальной сети «Одноклассники». При этом информация просто размещается на сайте. Можно ли в таком случае размещение информации о заведомо ложном сообщении об акте терроризма квалифицировать по ст. 207 УК РФ?

В науке уголовного права не разрешен вопрос о том, могут ли быть адресатами такого сообщения граждане, в функциональные обязанности которых не входит принятие мер по предотвращению террористического акта.

По мнению одной группы специалистов, адресатами заведомо ложного сообщения об акте терроризма не могут быть граждане, на которых не лежит правовая обязанность предпринимать меры к предотвращению готовящегося террористического акта[1].

Другая группа специалистов считает, что адресатами ложных сообщений могут быть не только органы государственной власти или органы местного самоуправления, но также должностные лица и сотрудники учреждений, предприятий и организаций, интересы которых могут пострадать при реальном совершении действий,

[1] Уголовное право России. Часть Особенная : учеб. для вузов / Б. В. Волженкин [и др.] ; отв. ред. Л. Л. Кругликов. 2-е изд., перераб. и доп. М., 2004. С. 441.

фигурирующих в сообщении; ложное сообщение может быть адресовано и частному лицу[1].

Представляется, что с учетом повышенной степени общественной опасности рассматриваемого преступления адресатами заведомо ложного сообщения об акте терроризма могут выступать не только государственные и муниципальные органы и учреждения, организации независимо от форм собственности, но и граждане. Однако изучение судебных приговоров не выявило ни одного случая направления заведомо ложного сообщения об акте терроризма конкретному гражданину.

Ст. 207 УК РФ предусматривает ответственность за заведомо ложное сообщение:

1) о взрыве – процессе освобождения большого количества энергии в ограниченном объеме за короткий промежуток времени. В результате взрыва вещество, заполняющее объем, в котором происходит освобождение энергии, превращается в сильно нагретый газ с очень высоким давлением. Этот газ с большой силой воздействует на окружающую среду, вызывая ее движение. Взрыв в твердой среде сопровождается ее разрушением и дроблением[2];

2) о поджоге – возгорании в результате умышленных или неосторожных действий, после чего пожар распространяется самопроизвольно[3];

3) об иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий.

Законодатель не уточняет круг «иных действий», что позволяет говорить о том, что данное понятие является оценочным. Оценочные понятия УК РФ – это понятия, содержание которых в уголовном законе не конкретизировано и определяется правоприменителем с учетом фактических обстоятельств уголовного дела. В настоящее время в УК РФ насчитывается 160 разновидностей оценочных понятий, которые включены в содержание 260 статей. Уголовный закон не раскрывает содержания оценочных понятий. Их толкование лежит за его пределами, что и позволяет относить нормы, при конструировании которых они используются, к неопределенным.

---

[1] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. И. Чучаева. 2-е изд., испр., доп. и перераб. М., 2010. С. 325.

[2] Большая советская энциклопедия // Словари онлайн : сайт. URL: https://bse.slovaronline.com/6242-VZRYV (дата обращения: 15.07.2023).

[3] *Сухарев А. Я., Крутских В. Е., Сухарева А. Я.* Большой юридический словарь // Словари онлайн : сайт. URL: https://rus-jur-terms.slovaronline.com/4766-ПОДЖОГ (дата обращения: 15.07.2023).

Использование оценочных понятий как прием законодательной техники известен отечественному законодательству на протяжении всей его многовековой истории.

Верховный Суд Российской Федерации в постановлении от 9 февраля 2012 г. № 1 рекомендует понимать под иными действиями действия, сопоставимые по последствиям со взрывом или поджогом, например устройство аварий на объектах жизнеобеспечения; разрушение транспортных коммуникаций; заражение источников питьевого водоснабжения и продуктов питания; распространение болезнетворных микробов, способных вызвать эпидемию или эпизоотию; радиоактивное, химическое, биологическое (бактериологическое) и иное заражение местности; вооруженное нападение на населенные пункты, обстрелы жилых домов, школ, больниц, административных зданий, мест дислокации (расположения) военнослужащих или сотрудников правоохранительных органов; захват и (или) разрушение зданий, вокзалов, портов, культурных или религиозных сооружений.

Изучение правоприменительной практики показало, что заведомо ложно сообщают следующую информацию: «в магазине "Лента" в ячейке 118 лежит бомба, состоящая из Е400, Е40, а также хлористого кальция», «взорву аэропорт в Архангельске, если не приедут за посылкой, Иншааллах», «в здании вашей школы заложена бомба, которая придет в действие в течение полутора часов. Мои требования, при которых бомба не будет активирована,...», «я *The Race* из группировки *Andromeda*, предупреждаю вас о том, что завтра с 11:02 по 11:09 к зданию центра помощи детям прилетят беспилотники, к которым будут прикреплены взрывчатые устройства», «в здании заложено 30 бомб, которые активируются через 5 часов после отправки данного сообщения» и т. д.

2. Сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий должно быть ложным, т. е. не соответствующим действительности. Направляя такое сообщение, лицо точно знает, что оно не соответствует действительности.

Ч. 2 ст. 207 УК РФ предусматривает ответственность за заведомо ложное сообщение об акте терроризма в отношении объектов социальной инфраструктуры либо повлекшее причинение крупного ущерба.

В соответствии с примечанием 2 к ст. 207 УК РФ под объектами социальной инфраструктуры понимаются организации систем здравоохранения, образования, дошкольного воспитания,

предприятия и организации, связанные с отдыхом и досугом, сферы услуг, пассажирского транспорта, спортивно-оздоровительные учреждения, система учреждений, оказывающих услуги правового и финансово-кредитного характера, а также иные объекты социальной инфраструктуры.

Перечень объектов социальной инфраструктуры является открытым, так как законодатель, описывая виды таких объектов, воспользовался законодательной конструкцией «иные объекты инфраструктуры».

Слово «инфраструктура» произошло от английского *infrastructure* – «основание, фундамент». В финансовом словаре[1] социальная инфраструктура определяется как группа обслуживающих отраслей и видов деятельности, призванных удовлетворять потребности людей; гарантировать необходимый уровень и качество жизни; обеспечивать воспроизводство человеческих ресурсов и профессионально подготовленных кадров для всех сфер национальной экономики.

Понятие «социальная инфраструктура» и ее функционирование относится к отечественной экономической науке, которая в 70–80-х гг. XX в. стала использовать это понятие[2].

Социальная инфраструктура обеспечивает жизнедеятельность населения на территории его проживания посредством предоставления услуг жилищно-коммунального хозяйства, пассажирского транспорта, здравоохранения, образования, культуры, спорта и других социальных комплексов.

Социальная инфраструктура включает три основных понятия: совокупность объектов инфраструктуры, условия их формирования и функционирования, обеспечивающие определенный уровень качества жизни населения на конкретной территории.

В науке существует точка зрения, согласно которой социальная инфраструктура включает в себя все объекты, удовлетворяющие потребности человека, начиная от жилья и заканчивая объектами культуры[3].

Специального закона, в котором были бы определены объекты социальной инфраструктуры, нет. Существуют отдельные нормы

---

[1] Финансовый словарь // Академик : сайт. URL: https://dic.academic.ru/dic.nsf/fin_enc/29549 (дата обращения: 15.07.2023).

[2] *Важенин С. Г.* Социальная инфраструктура народнохозяйственного комплекса. М., 1984.

[3] *Сычева И. В., Сычева Н. А.* Исследование содержания категории «социальная инфраструктура» // Известия Тульского государственного университета. Экономические и юридические науки. 2012. № 2–1. С. 230–238.

в законах или иных правовых актах, толкование которых позволяет определить круг таких объектов. Так, например, Федеральный закон от 24 ноября 1995 г. № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»[1] содержит перечень объектов социальной инфраструктуры, к которым отнесены жилые здания.

В распоряжении Правительства Российской Федерации от 19 августа 2020 г. № 2134-р «Об утверждении перечня объектов социальной инфраструктуры, проектная документация на строительство, реконструкцию которых в соответствии с подпунктом 7.8 статьи 11 Федерального закона "Об экологической экспертизе" не является объектом государственной экологической экспертизы»[2] приводится перечень объектов социальной инфраструктуры. Этот перечень шире, чем перечень, содержащийся в примечании к ст. 207 УК РФ. Кроме того, каждый регион имеет свой реестр объектов социальной инфраструктуры и услуг, например Реестр объектов социальной инфраструктуры и услуг в приоритетных сферах жизнедеятельности инвалидов и других маломобильных групп населения Свердловской области.

Изучение материалов правоприменительной практики показывает, что объектами социальной инфраструктуры считают здания кафе, магазинов, стадионы, аэропорты. Однако ФКУ ИК-4 УФСИН России по Новгородской области, а также жилой дом в г. Курчатове не были признаны объектами социальной инфраструктуры[3].

Таким образом, понятие «социальная инфраструктура» является оценочным при определении «иных объектов социальной инфраструктуры». С учетом признака «социальная» к ним можно отнести любые объекты, удовлетворяющие потребности человека, в том числе, например, и кладбище.

---

[1] О социальной защите инвалидов в Российской Федерации : Федер. закон № 181-ФЗ : принят Гос. Думой 20 июля 1995 г. : одобрен Советом Федерации 15 нояб. 1995 г. : в ред. от 28 дек. 2022 г. // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 15.07.2023). Режим доступа: для зарегистрир. пользователей.

[2] Об утверждении перечня объектов социальной инфраструктуры, проектная документация на строительство, реконструкцию которых в соответствии с подпунктом 7.8 статьи 11 Федерального закона «Об экологической экспертизе» не является объектом государственной экологической экспертизы : распоряжение Правительства Рос. Федерации от 19 авг. 2020 г. № 2134-р : в ред. от 30 окт. 2021 г. // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 15.07.2023). Режим доступа: для зарегистрир. пользователей.

[3] *Ковлагина Д. А.* Проблемы дифференциации ответственности за заведомо ложное сообщение об акте терроризма // Уголовное право. 2019. № 6. С. 46–50.

В целях исключения проблем, возникающих в правоприменительной практике при отнесении тех или иных объектов к объектам социальной инфраструктуры, что влияет на квалификацию преступления, предусмотренного ст. 207 УК РФ, необходимо закрепить единое толкование объектов социальной инфраструктуры постановлением Верховного Суда Российской Федерации.

Ч. 2 ст. 207 УК РФ также предусматривает ответственность за заведомо ложное сообщение об акте терроризма, повлекшее крупный ущерб, под которым понимается ущерб, сумма которого превышает один миллион рублей. Изучение судебной практики показало, что при осуждении по ч. 2 на обвиняемого не возлагается обязанность возмещения причиненного ущерба. Это связано с тем, что при возбуждении уголовного дела никто не признается потерпевшим.

Неоднозначность подходов в теории уголовного права и в правоприменительной практике к признанию потерпевшим государства дает основание предложить при совершении преступления, предусмотренного ст. 207 УК РФ, признавать потерпевшим государство в лице территориальных органов Федерального казначейства, так как именно государственные структуры (МВД России, ФСБ России) проводят проверку объектов в связи с поступлением ложного сообщения об акте терроризма и несут финансовые затраты в ходе ее проведения.

Кроме того, если в результате эвакуации причиняется материальный ущерб коммерческим организациям (торгово-развлекательные центры, объекты туристской инфраструктуры и пр.), то имеются основания признавать их потерпевшими.

Ч. 3 ст. 207 УК РФ предусматривает ответственность за заведомо ложное сообщение об акте терроризма в целях дестабилизации деятельности органов власти (данный признак будет раскрыт в субъективной стороне).

Ч. 4 ст. 207 УК РФ предусматривает ответственность за заведомо ложное сообщение об акте терроризма, повлекшее по неосторожности смерть человека или иные тяжкие последствия. Термин «иные тяжкие последствия» достаточно часто используется при конструировании норм Особенной части УК РФ. Этот термин является оценочным и, как правило, разъясняется Пленумом Верховного Суда Российской Федерации применительно к конкретным преступлениям. Так, в постановлении Пленума Верховного Суда Российской Федерации от 16 октября 2009 г. № 19 закреплено положение о том, что под тяжкими последствиями следует понимать ... крупные аварии и длительную остановку транспорта или производственного процесса, иное нарушение деятельности организа-

ции, причинение значительного материального ущерба, причинение смерти по неосторожности, самоубийство или покушение на самоубийство потерпевшего и т. п.[1] По конструкции объективной стороны состав преступления, предусмотренный ст. 207 УК РФ, является формальным (ч. 1, 3), материальным (ч. 2, 4).

Субъективная сторона ст. 207 УК РФ – умышленная форма вины. Вид умысла – прямой. Прямой умысел означает, что лицо осознавало общественную опасность такого своего действия, как заведомо ложное сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, и желало осуществить именно такое действие. Лицо должно осознавать, что оно сообщает заведомо ложные сведения, т. е. сведения, не соответствующие действительности, о чем оно достоверно знает. Если лицо добросовестно заблуждается на счет истинности сообщаемых сведений, то его действия не подлежат квалификации по ст. 207 УК РФ.

Факультативный признак субъективной стороны ст. 207 УК РФ – мотив и цель – становятся обязательными.

Ч. 1 ст. 207 УК РФ предусматривает совершение этого преступления из хулиганских побуждений. Хулиганство выступает мотивом совершения преступления.

Хулиганский мотив толкуется Пленумом Верховного Суда Российской Федерации как умышленное нарушение общепризнанных норм и правил поведения[2]. При этом «поведение виновного является открытым вызовом общественному порядку и обусловлено желанием противопоставить себя окружающим, продемонстрировать пренебрежительное к ним отношение»[3].

Ч. 3 ст. 207 УК РФ предусматривает специальную цель – дестабилизация деятельности органов власти. Цель – дестабилизация деятельности органов власти – не раскрывается, хотя и используется.

---

[1] О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий : постановление Пленума Верховного Суда Рос. Федерации от 16 окт. 2009 г. № 19 : в ред. от 11 июня 2020 г. // СПС КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_93013/ (дата обращения: 15.07.2023).

[2] О судебной практике по уголовным делам о хулиганстве и иных преступлениях, совершенных из хулиганских побуждений : постановление Пленума Верховного Суда Рос. Федерации от 15 нояб. 2007 г. № 45 // Рос. газ. 2007. № 260.

[3] О судебной практике по делам об убийстве (ст. 105 УК РФ) : постановление Пленума Верховного Суда Рос. Федерации от 27 янв. 1999 г. № 1 : в ред. от 3 марта 2015 г. // СПС КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_21893/ (дата обращения: 15.07.2023).

Например в Военной доктрине Российской Федерации[1], Стратегии национальной безопасности Российской Федерации[2] сказано, что в целях дестабилизации общественно-политической ситуации в Российской Федерации распространяется недостоверная информация, в том числе заведомо ложные сообщения об угрозе совершения террористических актов. В информационно-телекоммуникационной сети Интернет размещаются материалы террористических и экстремистских организаций, призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершению самоубийства, а также осуществляется пропаганда криминального образа жизни, потребления наркотических средств и психотропных веществ и т. д.

Верховный Суд Российской Федерации в постановлении от 9 февраля 2012 г. № 1 дает следующие рекомендации: «Обратить внимание судов на то, что цели дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений являются обязательным признаком террористического акта (статья 205 УК РФ). При решении вопроса о направленности умысла виновного лица на дестабилизацию деятельности органов власти или международных организаций следует исходить из совокупности всех обстоятельств содеянного и учитывать, в частности, время, место, способ, обстановку, орудия и средства совершения преступления, характер и размер наступивших или предполагаемых последствий, а также предшествующее преступлению и последующее поведение виновного».

Таким образом, все вышеперечисленные действия могут быть отнесены к дестабилизации.

Субъект ст. 207 УК РФ – физическое вменяемое лицо, достигшее 14-летнего возраста.

Отграничение ст. 207 УК РФ от смежных составов

Отграничение ч. 1 от ч. 2 ст. 207 УК РФ.

Изучение правоприменительной практики показало, что встречаются ситуации, когда заведомо ложное сообщение касается нескольких объектов, часть из которых относится к объектам социальной инфраструктуры, а другие – нет. Возникает проблема – какую часть

[1] Военная доктрина Российской Федерации : утв. Президентом Рос. Федерации от 25 дек. 2014 г. № Пр-2976 // Рос. газ. 2014. № 298.

[2] О Стратегии национальной безопасности Российской Федерации : Указ Президента Рос. Федерации от 2 июля 2021 г. № 400 // Собр. законодательства Рос. Федерации. 2021. № 27 (ч. II). Ст. 5351.

статьи (ч. 1 или ч. 2) применять. В этом случае следует руководствоваться правилами квалификации при конкуренции уголовно-правовых норм, согласно которым при конкуренции различных частей одной статьи действия виновного подлежат квалификации лишь по той части, по которой предусмотрено более строгое наказание[1].

Отграничение ст. 207 УК РФ «Заведомо ложное сообщение об акте терроризма» от ст. 205 УК РФ «Террористический акт».

Диспозиция ч. 1 ст. 205 УК РФ предусматривает в качестве одного из признаков объективной стороны угрозу совершения террористического акта.

В науке уголовного права существует несколько точек зрения на данную проблему. По мнению А. Бриллиантова[2], заведомо ложное сообщение об акте терроризма отличается от террористического акта по форме угрозы а именно по признаку реальности угрозы: если угроза реальна, виновный намеревается привести ее в исполнение и имеет реальную возможность сделать это, то содеянное является террористическим актом. По мнению ряда авторов, не имеет уголовно-правового значения, была ли угроза объективно реальной (т. е. предпринимались ли конкретные действия, направленные на приготовление к реализации угрозы, и намеревался ли виновный вообще исполнить угрозу). Заведомо ложное сообщение об акте терроризма следует отграничивать от террористического акта по такому признаку состава преступления, как цель[3].

По мнению Г. В. Овчинниковой, следует разграничивать угрозу совершения террористического акта и состав ст. 207 УК РФ по трем признакам:

1. Угрозу, предусмотренную ч. 1 ст. 205 УК РФ, высказывают сами террористы. Заведомо ложное сообщение исходит от других лиц.

2. Мотивы и цели действий, предусмотренных ст. 207 и 205 УК РФ, различны. Действия, перечисленные в ст. 205 УК РФ, направлены на запугивание населения, на оказание воздействия на принятие решений органами власти. Преступление, охватываемое ст. 207 УК РФ, возможно из хулиганских побуждений как легкомысленное проявление подросткового озорства и не преследует

---

[1] О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда Рос. Федерации от 27 дек. 2002 г. № 29 : в ред. от 15 дек. 2022 г. // СПС КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_40412/ (дата обращения: 15.07.2023).

[2] *Бриллиантов А.* Заведомо ложный донос: вопросы квалификации // Уголовное право. 2014. № 3. С. 22–26.

[3] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Г. А. Есаков [и др.] ; под ред. Г. А. Есакова. М., 2017.

целей повлиять на принятие решений органами власти или международными организациями.

3. Последствия террористического акта включены в элементы объективной стороны его состава (в ч. 1 – в виде опасности, в ч. 3 – в виде реального воплощения опасности в различные последствия). Состав преступления, предусмотренного ст. 207 УК РФ, – чисто формальный[1].

Информация о действиях, образующих террористический акт, не обязательно должна быть истинной, реальной. Такой вывод можно сделать, проведя аналогию со ст. 119 УК РФ. Ответственность по данной статье наступает только в случае, если имелись основания опасаться реализации этой угрозы, при этом у виновного может и не быть желания привести угрозу в исполнение. Таким образом, при разграничении ст. 205 и 207 УК РФ следует делать акцент на цель совершения преступления.

Кроме того, как правильно отмечает Г. В. Овчинникова, угрозу совершить теракт высказывают сами террористы, а «заведомо ложное сообщение об угрозе взрыва, поджога и т. д. исходит от других лиц, информирующих о якобы подготавливаемых кем-то террористических действиях»[2].

Отграничить друг от друга данные преступления можно по субъективной стороне. В ст. 207 УК РФ отсутствует указание на цель воздействия на принятие решений органами власти или международными организациями. Если виновный сообщает о готовящемся акте терроризма и предъявляет определенные требования к органам власти или международным организациям (например о передаче денег) как условие несовершения им взрыва или поджога (т. е. действует в целях воздействия на принятие решений органами власти или международными организациями) и адресатами данная угроза воспринимается реально (даже если преступник и не намеревался привести ее в исполнение), то содеянное следует квалифицировать не по ст. 207, а по ст. 205 УК РФ.

Безусловно, степень общественной опасности терроризма и заведомо ложного сообщения об акте терроризма выше в случае совершения этого преступления в условиях проведения специальной военной операции либо в условиях чрезвычайного положения, стихийного или иного общественного бедствия, а также при массовых беспорядках, в условиях вооруженного конфликта или военных действий.

---

[1] *Овчинникова Г. В.* Терроризм. Сер. «Современные стандарты в уголовном праве и уголовном процессе» / науч. ред. Б. В. Волженкин. СПб., 1998. С. 28.

[2] *Овчинникова Г. В.* Указ. соч. С. 29.

В настоящее время такие события не влияют на квалификацию, но учитываются судом при назначении наказания как обстоятельство, отягчающее наказание (ст. 63 УК РФ). Представляется, что это не совсем правильно, так как события, перечисленные выше, повышают степень общественной опасности рассматриваемых преступлений.

Для реализации принципа справедливости (ст. 6 УК РФ) возможно дополнить ст. 207 УК РФ ч. 3.1 следующего содержания: «Деяние, предусмотренное ч. 1–3 настоящей статьи, совершенное в условиях чрезвычайного положения, стихийного или иного общественного бедствия, а также при массовых беспорядках, в условиях вооруженного конфликта, специальной военной операции или военных действий».

Отграничение заведомо ложного сообщения об акте терроризма от вымогательства.

В теории уголовного права существуют определенные проблемы при выборе уголовно-правовой нормы тогда, когда способ выступает в качестве самостоятельного деяния, которое посягает на свой объект уголовно-правовой охраны и признается в соответствующей норме УК РФ самостоятельным преступлением, а в данном случае самостоятельное деяние выступает способом совершения преступления.

Несколько лет назад в России появилась новая форма вымогательства – «телефонный терроризм». Вымогая деньги у предпринимателей, злоумышленники обещают совершить звонок в правоохранительные органы с заведомо ложным сообщением о том, что в помещении, принадлежащем настоящей организации, находится взрывчатка.

В ст. 163 УК РФ «Вымогательство» данное преступление закреплено как требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких. Так же как и при заведомо ложном сообщении об акте терроризма, вымогательство представляет собой в том числе угрозу распространения иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего, хотя и без уточнения способа осуществления этой угрозы.

Для того чтобы привлечь виновного к уголовной ответственности, необходимо прежде всего установить, что обещание сделать

звонок о «заложенной бомбе» воспринимается потерпевшим как реальное, т. е. у него должны быть основания опасаться осуществления этой угрозы. По мнению Л. Д. Гаухмана и С. В. Максимова, угроза запугивания совершением перечисленных в ст. 163 УК РФ действий должна быть наличной, т. е. выражаться в устной или письменной форме, и реальной, т. е. восприниматься потерпевшим в качестве осуществимой[1]. Обещание сообщить «о заложенной бомбе» является способом совершения преступления, полностью охватывается ст. 163 УК РФ, и дополнительной квалификации по другим статьям УК РФ не требуется.

На практике встречаются ситуации, когда лицо совершает вымогательство под угрозой распространения иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего, а затем в связи с невыполнением потерпевшим требований реализует свою угрозу, осуществляя звонок и сообщая о «заложенной бомбе». По действующим правилам содеянное следует квалифицировать по совокупности преступлений (вымогательство и заведомо ложное сообщение об акте терроризма). В данном случае можно говорить о реальной совокупности преступлений, когда одно преступление является своеобразным следствием другого преступления, обусловлено первым преступлением.

Отграничение ст. 207 УК РФ от ст. 306 УК РФ «Заведомо ложный донос».

Отграничение заведомо ложного сообщения об акте терроризма (ст. 207 УК РФ) от заведомо ложного доноса (ст. 306 УК РФ) можно провести по следующим основным признакам:

Родовой объект ст. 207 УК РФ – это общественные отношения в сфере обеспечения общественной безопасности и общественного порядка, или иначе – общественные отношения в сфере обеспечения общественной безопасности в широком смысле слова. Родовой объект ст. 306 УК РФ – это общественные отношения в сфере обеспечения стабильности и нормального функционирования государственной власти.

Видовой объект ст. 207 УК РФ – это общественные отношения в сфере обеспечения общественной безопасности в узком смысле слова. Видовой объект ст. 306 УК РФ – это общественные отношения в сфере обеспечения осуществления правосудия.

Объективная сторона ст. 207 УК РФ заключается в заведомо ложном сообщении о готовящихся взрыве, поджоге или иных дей-

[1] *Гаухман Л. Д., Максимов С. В.* Ответственность за преступления против собственности. 2-е изд., испр. М., 2001. С. 121.

ствиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Объективная сторона ч. 1 ст. 306 УК РФ выражается в заведомо ложном доносе об уже совершенном преступлении.

Таким образом, уголовная ответственность по ст. 207 УК РФ наступает только в случае, если лицо сообщает о готовящемся акте терроризма. В этой связи не влекут уголовной ответственности по ст. 207 УК РФ заведомо ложные сообщения о якобы уже совершенных актах терроризма или намерении определенных лиц совершить такой акт. В подобном случае ответственность наступает за заведомо ложный донос по ст. 306 УК РФ.

Кроме того, при заведомо ложном сообщении об акте терроризма лицо, сообщившее об этом, неизвестно и его розыск, как правило, затруднен. При заведомо ложном доносе лицо, сделавшее сообщение, известно и сообщает ложные сведения официально.

Так, например, гражданин Краснов, находясь в здании ОП № 4 МУ МВД России «Оренбургское», будучи предупрежденным об уголовной ответственности по ст. 306 УК РФ, подал заведомо ложное заявление о том, что неизвестное лицо неправомерно завладело принадлежащим ему автомобилем Kia Picanto. Однако в ходе доследственной проверки данный факт не нашел своего подтверждения. Гражданин Краснов был осужден по ч. 1 ст. 306 УК РФ.

В последнее время появился новый вид распространения заведомо ложной информации – сватинг – умышленное введение должностных лиц правоохранительных органов в заблуждение относительно личности лица, производящего заведомо ложное сообщение об акте терроризма.

Учитывая, что подобные сообщения не содержат просьбы о привлечении к ответственности определенного лица (проведении проверки в отношении него) и указания на предупреждение об уголовной ответственности по ст. 306 УК РФ, основания для дополнительной квалификации по ст. 306 УК РФ при таких обстоятельствах не усматриваются.

Вопросы для самоконтроля

1. Дайте определение понятию «заведомо ложное сообщение».
2. Назовите специалистов уголовного права, которые занимались проблемами уголовно-правового противодействия заведомо ложному сообщению об акте терроризма.
3. Перечислите проблемы, возникающие при квалификации заведомо ложного сообщения об акте терроризма.
4. Следовало бы законодателю усилить уголовную ответственность за заведомо ложное сообщение об акте терроризма, если деяние совершено в отношении объектов социальной инфраструктуры? Аргументируйте ответ.
5. К какой категории относится преступление, предусмотренное ч. 1 ст. 207 УК РФ?

Глава 2. Особенности механизма совершения заведомо ложных сообщений об актах терроризма

Изучение материалов уголовных дел, возбужденных по ст. 207 УК РФ в период с июня 2021 г. по июнь 2022 г., позволило выявить ряд закономерностей механизма совершения заведомо ложных сообщений об актах терроризма.

Способ совершения преступления.

В большинстве случаев (73 %) сообщения отправляются по электронной почте. Наиболее распространенными сервисами электронной почты для направления заведомо ложных сообщений об актах терроризма являются: *yandex.com*; *yandex.ru*; *gmail.com*; *ro.ru*; *mail.ru*; *hotmail.com*; *aol.com*. Реже – *protonmail.com*; *protonmail.ch*. Доступ к последним двум из указанных выше сервисов электронной почты на основании требования Генеральной прокуратуры Российской Федерации был ограничен Роскомнадзором 29 января 2020 г. Данные почтовые сервисы использовались злоумышленниками как в 2019 г., так и особенно активно в январе 2020 г. для рассылки под видом достоверных сведений ложных сообщений о массовом минировании объектов на территории Российской Федерации. На неоднократные запросы Роскомнадзора о предоставлении сведений для включения в реестр организаторов распространения информации в сети Интернет компания реагировала отказом. Сведения об администраторах почтовых ящиков, используемых для рассылки угроз, предоставлены не были.

Вместе с тем, несмотря на указанное выше ограничение, возможность доступа к информационным ресурсам *ProtonMail* с территории Российской Федерации существует с использованием сервисов VPN, технические особенности которых будут рассмотрены в главе 4 настоящей работы.

В 17 % случаев сообщение поступало посредством телефонной связи (при этом в 78 % – номер телефона был определен), реже – путем размещения сообщений в социальных сетях и направления сообщений посредством сервисов мгновенных сообщений (мессенджеров).

Чаще всего сообщение отправляется в то учреждение, в котором якобы должен произойти взрыв или иной акт терроризма. Как правило, это школы, детские сады, торговые центры, иные организации с массовым пребыванием людей. Администрации объектов транспортной инфраструктуры являются получателями подобных сообщений в 5 % изученных случаев.

Зачастую подобные сообщения поступают в правоохранительный орган (МВД России, ФСБ России, Росгвардию), иной государственный орган (МЧС России), органы местного самоуправления; общественные приемные политических деятелей или политических партий; средства массовой информации. При этом установлена следующая закономерность: сообщение, как правило, дублируется в различные правоохранительные органы. Для такого способа характерны направление нескольких сообщений с одного адреса, отправка одинакового текста с разных адресов, одинаковые имена почты, но разные домены.

Определенные предпосылки для роста числа заведомо ложных сообщений об актах терроризма, направляемых через формы обратной связи на официальных сайтах государственных органов, складываются в связи с тем, что большинство официальных сайтов не предполагают не только обязательную верификацию пользователей через портал «Госуслуги», но даже не имеют встроенного средства для получения *cookie*-файлов, благодаря которому можно было бы получить данные об устройстве и соединении злоумышленника.

В процессе исследования выявлены единичные случаи передачи сообщения через личное обращение, а также посредством факсимильной связи.

Анализ сообщений показывает, что в большинстве случаев (около 75 %) они не содержат каких-либо требований.

Примерно в 9 % случаев преступники демонстрируют корыстные мотивы – требуют перевести деньги на банковскую карту, номер телефона, электронный кошелек, а также криптовалюту.

В отдельных случаях (около 5 %) встречаются требования, направленные на получение максимального общественного резонанса: вызвать полицию, эвакуировать людей, сообщить в средства массовой информации, указать конкретные данные лиц (организации, взявшей ответственность), сжечь 1 млн руб. на центральной площади города, записать видео и выложить в Интернет.

Примерно в 10 % исследованных случаев преступники в сообщениях обозначают, что они передадут дальнейшие инструкции через свою страницу социальной сети, или информируют о необходимости ожидания получения последующих указаний. В единичных случаях выдвигаются требования зайти на определенный сайт в целях повышения рейтинга, получения голосов за клип в YouTube, возбуждения уголовного дела в отношении сотрудников правоохранительных органов.

До 24 февраля 2022 г. – начала специальной военной операции на территории Украины – требования политического характера, выдвигаемые злоумышленниками при передаче заведомо ложного сообщения об акте терроризма, являлись единичными (например, освободить лидера оппозиционеров, не проводить референдум и пр.). С началом специальной военной операции наблюдается резкий скачок числа подобных преступлений. При этом в сложившейся обстановке требования, выдвигаемые при передаче заведомо ложных сообщений об актах терроризма, в большей степени носят негативный эмоциональный окрас.

В 70 % случаев способ террористического акта, о котором содержится информация в сообщении, не конкретизирован: преступники используют общие фразы (заложена бомба, объект заминирован, заложено взрывное устройство или взрывчатое вещество и т. п.). В 7 % – содержатся указания на то, что взрывное устройство имеет механизм самоликвидации, который будет приведен в действие в случае неисполнения требований. В отдельных случаях (3,5 %) в сообщении содержится информация о наименовании конкретного взрывчатого вещества. Единичными являются случаи упоминания использования дронов.

Что касается времени совершения террористического акта (взрыва, поджога, совершения иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий), то в 56 % случаев время предполагаемого взрыва в сообщении вообще не указывается. В 20 % – указывается временной интервал после получения сообщения о готовящемся взрыве (например, в течение суток, определенного промежутка времени). Лишь в 5 % случаев обозначается точное время взрыва. Единичны случаи указания на конкретное событие, после которого произойдет взрыв: когда тронется поезд, взлетит самолет и пр.

В 34 % – информация в тексте сообщения содержала сведения о причастном к совершению преступления лице, либо данная информация содержалась в адресе электронной почты, с которой было отправлено сообщение, либо лицо представилось по телефону.

Личность преступника.

В процессе исследования выявлены три принципиально разные группы лиц, совершающие подобные преступления:

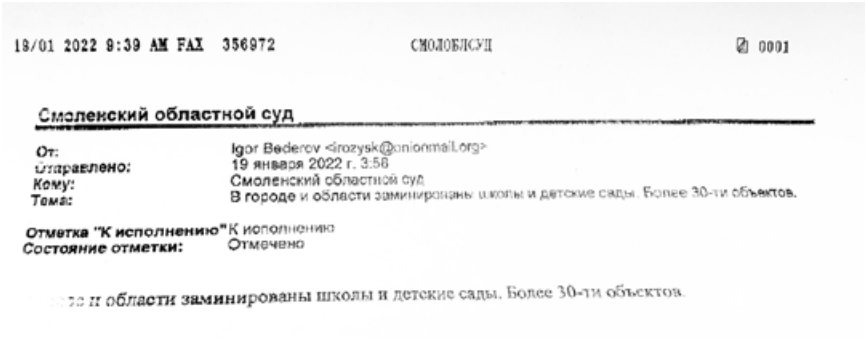
1) подростки – учащиеся общеобразовательных школ и колледжей (для сообщений характерно выдвижение требований не вызы-

вать оперативные службы; отсутствие материальных требований; объектами являются в большинстве случаев школы);

2) лица с провокационными склонностями и низкой социальной ответственностью, для которых мотивом чаще всего является стремление вызвать максимальный общественный резонанс;

3) представители криминальных колл-центров, находящиеся за пределами территории Российской Федерации, на профессиональной основе стремящиеся к оказанию информационно-психологического воздействия на государственные органы и население с целью вызвать панику и неуверенность.

Распространители ложных сообщений об акте терроризма могут использовать персональные данные, а также никнеймы третьих лиц для распространения своих угроз. Чаще всего это делается в качестве мести или в целях вымогательства денежных средств. В этом случае злоумышленник «подкидывает» правоохранительным органам возможность идентифицировать себя по никнейму, ФИО или иным признакам. Его конечная цель заключается в том, чтобы оперативные службы задержали подставляемое им лицо. На Западе такой прием известен под названием «сватинг», который был рассмотрен в главе 1 (рис. 1).


18/01 2022 9:39 AM FAX 356972 СМОЛОБЛСУД ☑ 0001

Смоленский областной суд

От: Igor Bederov <irozysk@onionmail.org>
Отправлено: 19 января 2022 г. 3:56
Кому: Смоленский областной суд
Тема: В городе и области заминированы школы и детские сады. Более 30-ти объектов.

Отметка "К исполнению" К исполнению
Состояние отметки: Отмечено

...е и области заминированы школы и детские сады. Более 30-ти объектов.

Рис. 1. Пример электронного письма, содержащего ложное сообщение о минировании, отправленного якобы от имени одного из авторов настоящей работы

Большинство подобных деяний совершается несовершеннолетними лицами в возрасте 10–15 лет. Часть их игнорируют наличие в сети Интернет своих ранее созданных аккаунтов в социальных сетях, оформленных на их настоящие данные. Обнаружение данных аккаунтов позволяет примерно в половине случаев успешно идентифицировать личности «минеров».

Характерно, что сватеры объединяются в сообщества в социальных сетях и мессенджерах. Эти сообщества часто публикуют сведения о «минируемых» объектах заранее. Между сообществами существует конкуренция, включая размещение в публичном доступе идентифицирующих данных на участников таких групп (рис. 2).

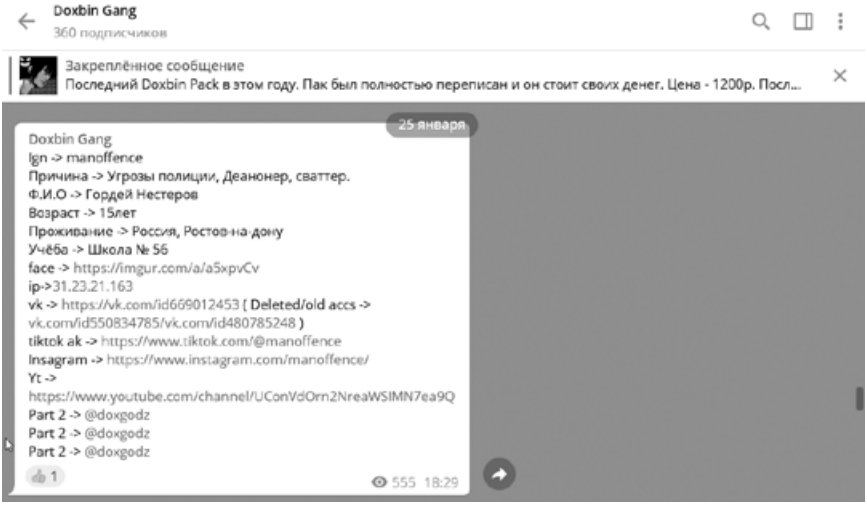


Рис. 2. Пример деанонимизации участника конкурирующего сообщества сватеров в сообществе *Doxbin Gang*

Многие сватеры сообщали о «минировании» собственных учебных заведений. В частности, это было в Екатеринбурге и Красноярске. Проведение опроса педагогов учебных заведений позволило выявить учащихся, склонных к девиантному поведению. Последующая проверка их аккаунтов и электронных устройств позволила подтвердить их причастность к распространению подобных сообщений.

Объектами заведомо ложных сообщений об актах терроризма являются места с массовым пребыванием людей. В большинстве случаев (33 %) это образовательные организации (школы, гимназии, лицеи). Детские сады значительно реже становятся объектами заведомо ложных сообщений об актах терроризма – в 4 % случаев. Примерно такое же количество случаев «минирования» колледжей, высших учебных заведений. Торговые объекты являлись объектами заведомо ложных сообщений об актах терроризма в 15 % случаев. В 10 % – объектом заведомо ложных сообщений об актах террориз-

ма являлось здание органа государственной власти, местного самоуправления. Причем здания правоохранительных органов выступали объектами «минирования» лишь в 2 % случаев. Высокую распространенность получили заведомо ложные сообщения об актах терроризма в отношении объектов транспортной инфраструктуры: здание аэропорта, самолет – 6 %, вокзал, станция метро, автовокзал – 5 %, общественный транспорт (поезд, поезд метро, электробус) – 1 %.

Среди социальных объектов выделяются больницы (5 %), объекты жизнеобеспечения – коммунальные предприятия (2 %), дома престарелых (1 %), детские дома (1 %).

Среди коммерческих организаций объектами заведомо ложных сообщений об актах терроризма в 3 % случаев являлись банки. Открытая местность выступает в качестве объекта заведомо ложных сообщений об актах терроризма лишь в 1 % случаев. Также среди объектов таких сообщений встречались жилые дома (3 %), гостиницы, исправительные учреждения, офисы компаний, театры, рестораны, отделения связи, музеи. Единичны случаи минирования центров помощи детям, а также пожарной безопасности. В 1 % – объектом преступного посягательства выступали отделение политической партии либо избирательные комиссии. Распространенность подобных объектов при заведомо ложных сообщениях об актах терроризма находится в пределах статистической погрешности.

Распространение ложных сообщений о минировании часто используется правонарушителями в целях вымогательства денежных средств у организаций, деятельность которых простаивает и теряет доход в связи с необходимостью проведения эвакуации и иных антитеррористических мероприятий. Это торговые центры, магазины, клубы, театры, кинотеатры и т. п.

Орудия и средства совершения преступлений.

Как указывалось выше, в настоящее время широкое распространение получила передача заведомо ложных сообщений об акте терроризма посредством современных цифровых технологий: с использованием электронной почты, социальных сетей, сервисов мгновенных сообщений, IP-телефонии с функцией подмены номера. Применительно к перечисленным выше интернет-сервисам общим является то, что организации, индивидуальные предприниматели и физические лица, являющиеся их владельцами и обеспечивающие их функционирование, обязаны соблюдать требования законодательства Российской Федерации, предъявляемые к организаторам распространения информации.

В соответствии со ст. 10.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1] организатором распространения информации в сети Интернет является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет.

Организаторы распространения информации обязаны осуществлять идентификацию своих пользователей, хранить в течение 6 месяцев текстовые сообщения своих пользователей, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения, а в течение 12 месяцев – информацию о фактах передачи данных сообщений, и предоставлять данную информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

Социальные сети представляют собой интерактивные многопользовательские сайты, контент (содержание) которых наполняется их посетителями с возможностью указания какой-либо информации об отдельном человеке, по которой аккаунт (страницу) пользователя смогут найти другие участники сети[2].

Под мессенджером понимается сервис в сети Интернет, предназначенный для обмена электронными сообщениями между пользователями.

IP-телефония отличается от привычной мобильной связи тем, что для ее использования не требуется телефонного аппарата (оконечного оборудования пользователя), идентификационного модуля абонента (сим-карты), а также подключения к базовой станции подвижной связи. Соединение устанавливается через специальное приложение по протоколу IP. При применении анонимайзеров установление реального IP-адреса, использованного для соединения, носит затруднительный характер.

---

[1] Об информации, информационных технологиях и о защите информации : Федер. закон № 149-ФЗ : принят Гос. Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. : в ред. от 31 июля 2023 г. // СПС КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 01.08.2023).

[2] *Чернец В., Базлова Т., Иванова Э.* Влияние через социальные сети / под общ. ред. Е. Г. Алексеевой. М., 2010. С. 29.

Следы.

Под следами преступления в криминалистике понимаются любые изменения окружающей среды, находящиеся в причинно-следственной связи с событием преступления. Для преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, характерно оставление в результате их совершения особой категории следов – цифровых. Под цифровыми следами понимаются результаты преобразования компьютерной информации в форме уничтожения, копирования, блокирования или модификации, а также соответствующие им изменения физических характеристик ее носителя, причинно связанные с событием преступления[1]. Заведомо ложное сообщение об акте терроризма не является исключением.

Существенные свойства цифровых следов:

1) относятся к категории материальных следов;

2) существуют исключительно на электронных носителях информации;

3) механизм их образования находится в зависимости от применяемой технологии записи информации на электронный носитель;

4) их возникновение детерминировано как технологическими процессами, возникающими в информационной системе при уничтожении, копировании, блокировании или модификации компьютерной информации, так и правовыми требованиями, предъявляемыми к субъектам, обеспечивающим функционирование информационно-телекоммуникационной инфраструктуры, и кредитно-финансовым организациям;

5) для их восприятия участниками расследования требуется их преобразование с использованием аппаратно-программного обеспечения.

К числу цифровых следов, позволяющих установить личность отправителя электронного сообщения, относятся: никнейм (сетевой псевдоним пользователя), адрес электронной почты и номер телефона, привязанный к нему при регистрации, фотография или аватар (изображение, графический объект), рекламные идентификаторы, геолокационная информация, данные о соединении и устройстве пользователя, платежные реквизиты, публичные переписки и участие в сообществах, иные связанные вебузлы и уникальные идентификаторы (рис. 3).

---

[1] *Гаврилин Ю. В., Гаспарян Г. З.* Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : учеб. пособие. М., 2021. С. 54.

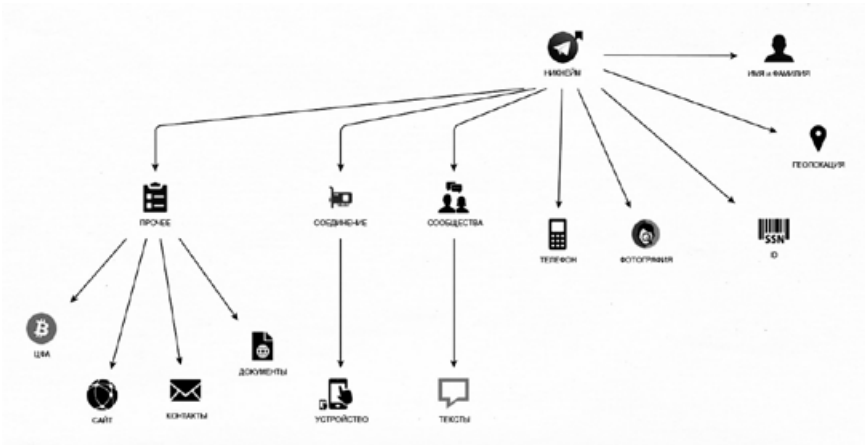


Рис. 3. Система цифровых идентификаторов личности

Совокупность перечисленных данных составляет обобщенный цифровой образ пользователя, включающий в себя индивидуальные, социальные и технические сведения, а также результат их анализа. Централизованный сбор и исследование цифрового образа личности представляют перспективное направление криминалистики и оперативно-розыскной деятельности. При этом в основе методологии исследования цифрового образа личности находятся методы анализа больших данных.

Говоря о цифровых следах в информационных системах, возникающих в процессе совершения заведомо ложных сообщений об акте терроризма, следует отметить их дуалистическую природу. С одной стороны, их возникновение обусловлено технологическими особенностями записи информации на соответствующий электронный носитель (карта памяти, флеш-накопитель, CD-диск, жесткий диск компьютера, встроенная память иного цифрового устройства). С другой стороны, возникновение цифровых следов связано с требованиями действующего законодательства к субъектам информационно-телекоммуникационной инфраструктуры. Так, как уже отмечалось выше, в соответствии с подп. 1 п. 4.2 ст. 10.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» организаторы распространения информации в сети Интернет обязаны осуществлять идентификацию своих пользователей по абонентскому номеру оператора подвижной радиотелефонной связи в порядке, установленном Правительством Российской

Федерации[1]. Кроме того, они обязаны хранить на территории Российской Федерации значительный объем сведений о передаваемых ими сообщениях и представлять уполномоченным государственным органам в установленном законом порядке.

Вопросы для самоконтроля

1. Сформируйте систему современных способов совершения заведомо ложных сообщений об актах терроризма.
2. Охарактеризуйте криминалистически значимые свойства личности преступника.
3. Дайте характеристику средств анонимизации, используемых при совершении преступления.
4. Укажите типичные следы, характерные для заведомо ложных сообщений об актах терроризма.

[1] Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями : постановление Правительства Рос. Федерации от 20 окт. 2021 г. № 1801 // СПС КонсультантПлюс : сайт. URL: http://www.consultant.ru (дата обращения: 22.08.2023). Режим доступа: для зарегистрир. пользователей.

Глава 3. Алгоритм действий следователя и сотрудников оперативных подразделений МВД России на этапе проверки и первоначальном этапе расследования заведомо ложных сообщений об актах терроризма

При рассмотрении сообщения о преступлении в порядке ст. 144 УПК РФ должностному лицу подразделения МВД России, которому поручено производство проверки (следователю, оперативному уполномоченному уголовного розыска или центра по противодействию экстремизму), необходимо выполнить комплекс проверочных мероприятий по установлению источника поступления заведомо ложного сообщения об акте терроризма (электронное сообщение, телефонный звонок) и события преступления, предусмотренного ст. 207 УК РФ. Данный комплекс мероприятий включает:

1) установление лица, принявшего сообщение об акте терроризма и передавшего информацию в уполномоченные органы власти (МВД России, ФСБ России, МЧС России и др.) (далее – заявитель), а также наименование и фактический адрес организации, в отношении которой было сделано данное сообщение;

2) получение объяснения от заявителя по обстоятельствам поступившего сообщения: содержание сообщения, способ его получения, дата и точное время поступления, адрес электронной почты или абонентский номер телефона, с которого и на который было отправлено сообщение (был совершен входящий вызов), либо на каком устройстве было прочитано сообщение электронной почты, наличие аналогичных фактов поступления сообщений;

3) в случае поступления сообщения посредством телефонной связи – предложение заявителю обратиться в офис компании оператора связи либо в личный кабинет абонента подвижной (мобильной) связи для получения информации о телефонных соединениях за период времени, соответствующий времени поступления сообщения, и приобщения ее к материалу проверки;

4) изучение представленной заявителем детализации, принимая во внимание при этом, что с учетом возможности технической подмены идентификатора вызывающего абонента (абонентского номера) в ней может быть указан иной номер, нежели тот, который увидел заявитель на своем устройстве (действительный номер, с которого был произведен телефонной вызов, либо IP-адрес);

5) осмотр места происшествия, в ходе которого:

– при наличии аудиозаписи телефонного разговора, во время которого передано сообщение об акте терроризма, изъять ее и обеспечить ее сохранность;

– осмотреть электронное сообщение об акте терроризма, зафиксировать его дословное содержание, установить время его поступления, наименование организатора распространения информации в сети Интернет, через которого передано электронное сообщение (далее – провайдер), приобщить сведения о технических данных (исходный код), хранящихся в его образе (оригинале, свойствах, заголовках), доменном имени электронного почтового провайдера (см. главу 4 настоящей работы);

6) установление лиц, организаций, органов государственной власти или местного самоуправления, которым причинен ущерб в связи с реагированием на заведомо ложное сообщение об акте терроризма, истребование в порядке ч. 4 ст. 21 УПК РФ документального подтверждения расходов (расчет суммы ущерба), установление лиц, наделенных правом представлять интересы организаций в органах внутренних дел, истребование доверенности, получение от них объяснения;

7) составление статистической карточки на выявленное преступление (форма № 1) и направление ее в информационный центр для учета.

После возбуждения уголовного дела необходимо выполнить следующий комплекс процессуальных действий, направленных на установление лица, совершившего преступление, и получение достаточных доказательств, дающих основание для предъявления ему обвинения в совершении преступления, предусмотренного ст. 207 УК РФ. Данный комплекс мероприятий включает:

1) уведомление заявителя о возбуждении уголовного дела (в случае возбуждения уголовного дела в отношении конкретного лица оно также подлежит уведомлению);

2) признание в качестве потерпевших физических лиц, организаций, государственных органов, органов местного самоуправления при установлении фактов причинения им материального ущерба в связи с реагированием на заведомо ложное сообщение об акте терроризма;

3) разъяснение представителю потерпевшего права требовать возмещения имущественного вреда, причиненного преступлением, путем подачи искового заявления, признание потерпевшего гражданским истцом;

4) в случае поступления сообщения посредством телефонной связи – допрос заявителя по обстоятельствам телефонного вызова, предполагающий:

– установление максимально точного содержания разговора: кем представился звонивший, какую информацию он сообщил, указывал ли в сообщении причину совершения акта терроризма и т. д.;

– подробное описание голоса (хриплый, высокий или низкий, молодой или старый, наличие иностранного акцента, регионального диалекта и т. д.); манеры строить фразы; характерных особенностей речи преступника (например, шепелявит, проглатывает окончание фразы, говорит скороговоркой и т. д.);

– выяснение наличия требований, суммы и способа передачи/перевода денежных средств (блиц-перевод, перевод на кошелек QIWI, криптовалюта и т. п.);

5) в случае поступления сообщения по электронной почте – установление круга пользователей компьютера или иного устройства, на которое пришло сообщение, обстоятельств его получения и содержания;

6) установление и допрос в качестве свидетелей очевидцев, должностных лиц, участвовавших в эвакуации, в том числе сотрудников охранных организаций, администраторов и т. д.;

7) получение в порядке, предусмотренном ст. 186.1 и 165 УПК РФ, на основании постановления суда информации у операторов мобильной связи[1] о соединениях между абонентами и (или) абонентскими устройствами: сведений о паспортных данных владельца абонентского номера, дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, об IMEI-коде абонентского устройства, сетевом трафике, IP-адресах, использованных для входа в личный кабинет мобильного оператора, о входящих и исходящих платежах по лицевому счету, номерах и месте расположения приемопередающих базовых станций, а также векторе (азимуте) направления сигнала[2];

---

[1] Установить принадлежность абонентского номера, звонившего оператору мобильной связи, возможно при помощи официального сайта Россвязи.

[2] Как правило, представлен в числовом выражении и означает угол, под которым находилось абонентское устройство по отношению к базовой станции в момент фиксации его активности в сети. Используя эти данные, можно создать графическую схему предполагаемого местонахождения подозреваемого лица, а при необходимости привлечь для этого сотрудника технической службы оператора связи.

8) запрос сведений об адресе торговой точки, продавце сим-карты, а также копии регистрационной документации при приобретении сим-карты;

9) при получении информации об IMEI-коде абонентского устройства, с которого производился исходящий вызов, содержащий заведомо ложное сообщение об акте терроризма – запрос сведений о всех сим-картах, использовавшихся на данном телефоне;

10) формирование и направление запросов в адрес организаторов распространения информации в сети Интернет: провайдеров, организаций, которым принадлежат социальные сети, почтовых сервисов, мессенджеров о предоставлении сведений, указанных при регистрации адреса электронной почты, создании аккаунта социальной сети или иного интернет-сервиса, посредством которого передано заведомо ложное сообщение об акте терроризма[1];

11) поручение подразделениям МВД России, осуществляющим оперативное сопровождение расследования (подразделениям уголовного розыска, подразделениям по противодействию экстремизму при взаимодействии с территориальными подразделениями БСТМ МВД России), выполнить следующие мероприятия:

– получить установочные данные лиц, на которых зарегистрированы либо использующих интересующие абонентские номера связи и адреса электронной почты, а также определить местонахождение абонента связи либо отправителя сообщения по электронной почте по геолокации;

– проверить возможную причастность фигурантов к указанной противоправной деятельности, осуществить проверку по информационным ресурсам МВД России в целях установления их личности, а также иных сведений, представляющих оперативный интерес;

– осуществить проверку информации об использованном при совершении преступления адресе электронной почты, IP-адресе, абонентском номере пользователя услугами связи и иных полученных

[1] Действующая практика позволяет на основании запроса о предоставлении сведений получать без судебного разрешения информацию об абоненте с указанием его установочных данных, о номере и дате заключенного договора об оказании телеметрических услуг с приложением заверенной копии договора и протоколы работы в сети Интернет (*log*-файлы), а также информацию об IP-адресах, с которых осуществлялось создание и администрирование аккаунта, работа электронной почты, об абонентах, которым в указанный момент времени выдавался установленный IP-адрес, о MAC-адресах компьютерной техники и сетевого оборудования, с использованием которых осуществлялся доступ к сети Интернет.

на данном этапе расследования сведений по ведомственным автоматизированным информационно-поисковым системам и банкам данных для рассмотрения вопроса о соединении уголовных дел;

– получить информацию о паспортных данных, абонентских номерах, электронной почте, IP-адресах, использованных для регистрации пользователя/аренды хостинга, для входа в личный кабинет или панель управления для администрирования, об оплате услуг регистрации и аренды с указанием полных реквизитов плательщика, провести анализ *cookie*-файлов в организациях-арендодателях хостинга и организациях-регистраторах доменных имен[1];

– установить наличие видеонаблюдения в месте расположения компьютерного оборудования, при помощи которого было совершено преступление;

– установить операции по указанному в сообщении электронному кошельку (при наличии), включая операции зачисления, перевода денежных средств, пополнения через терминалы или банкоматы;

– в случае технической подмены идентификатора вызывающего абонента установить у оператора связи входящего звонка технические реквизиты звонка, при использовании IP-телефонии – запросить IP-адрес регистрации и авторизаций, а также способы оплаты;

12) при установлении факта географического месторасположения интернет-провайдеров, организаций, которым принадлежат социальные сети, почтовые и иные интернет-сервисы на территории иностранного государства – направление запроса в территориальное подразделение Национального центрального бюро Интерпола МВД России на региональном уровне в соответствии с требованиями Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола, утвержденной приказом МВД России от 6 октября 2006 г. № 786, в целях получения сведений об адресе электронной почты, аккаунте социальной сети и иного интернет-сервиса, посредством которого передано сообщение об акте терроризма;

13) при установлении подразделениями МВД России, осуществляющими оперативное сопровождение расследования, факта наличия видеонаблюдения в месте совершения преступления – проведение выемки видеозаписи;

[1] В целях установления организации-регистратора доменного имени необходимо воспользоваться интернет-ресурсом www.reg.ru.

14) при получении сведений о лицах, на которых зарегистрированы абонентские номера, привязанных к ним банковских картах, электронных почтовых ящиках, аккаунтах и иных ресурсах – незамедлительное направление поручения (в случае регистрации на территории иного субъекта Российской Федерации) на имя руководителя следственного подразделения о проведении допросов данных лиц, выемки документов, подтверждающих открытие/регистрацию в информационных и банковских ресурсах, при необходимости – изъятие образцов почерка;

15) проведение иных следственных и процессуальных действий в соответствии со складывающейся следственной ситуацией по уголовному делу с учетом имеющейся информации и доказательств.

Вопросы для самоконтроля

1. Приведите комплекс мероприятий, направленных на установление события преступления.
2. Приведите комплекс мероприятий, направленных на установление лица, совершившего преступление.
3. Раскройте предмет и содержание взаимодействия участников расследования заведомо ложных сообщений об актах терроризма.

Глава 4. Методы и средства получения и анализа информации из открытых источников, используемые для установления личности отправителей заведомо ложных сообщений об актах терроризма

Как отмечалось выше, не всегда данные о пользователях сервисов электронной почты, социальных сетей и мессенджеров, устанавливаемые на основе сведений о пользователях абонентских номеров операторов подвижной радиотелефонной связи, указываемых при регистрации учетных записей пользователей, носят достоверный характер. В ряде случаев абонентский номер бывает зарегистрирован либо на юридическое лицо, либо на умершее лицо, либо оператор связи может указанными сведениями не располагать по иным причинам. В таких случаях необходимо воспользоваться технологией OSINT (англ. *Open Source INTelligence* – разведка по открытым источникам) – комплексной областью знаний, направленной на поиск, сбор и обработку информации из общедоступных источников.

К числу задач, разрешаемых в процессе расследования ***заведомо ложных сообщений об актах терроризма, отправленных по электронной почте***, относятся:

1. Проверка фактического существования того почтового ящика, с которого было направлено сообщение. С указанной целью производится направление SMTP-запроса[1] к почтовому серверу отправителя, который позволяет установить факт регистрации электронного почтового ящика, с использованием которого осуществлялась отправка сообщения. В последующем это дает возможность направить в адрес организации – владельца сервиса электронной почты или ее российского представительства – запрос о предоставлении информации, указанной при создании электронного почтового ящика.

В качестве примеров сервисов, позволяющих проводить SMTP-запросы в целях подтверждения существования электронного почтового ящика отправителя, можно назвать:

https://mailboxlayer.com/;

https://2ip.ru/mail-checker/;

https://ivit.pro/services/email-valid/.

2. Анализ служебных заголовков сообщения. Каждое электронное сообщение, передаваемое через сервис электронной почты,

[1] SMTP (*Simple Mail Transfer Protocol*) – сетевой протокол, предназначенный для передачи электронной почты.

сохраняет в себе информацию о тех сетевых узлах, через которые оно проходило до получения его пользователем сервиса электронной почты. Эти сведения сохраняются в служебных заголовках электронного сообщения. Служебный заголовок – это набор служебной информации, содержащий адрес отправителя и получателя, маршрут движения письма, вид кодировки, тему письма, а также служебные метки, оставленные программными средствами защиты от вредоносного программного обеспечения и массовых рассылок[1] (рис. 4, 5, 6, 7).

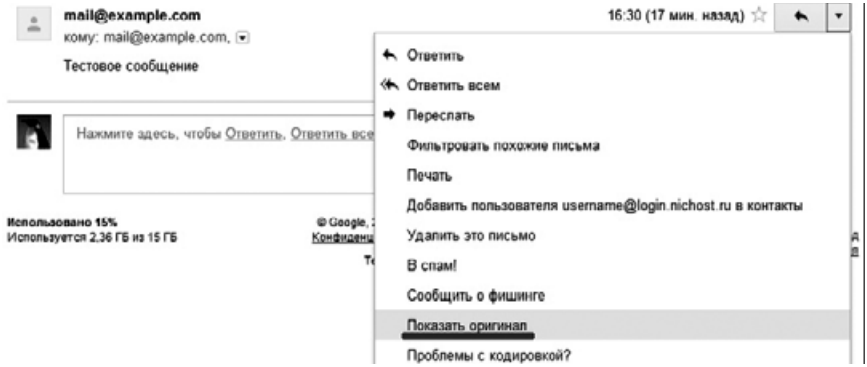


Рис. 4. Поиск служебных заголовков сообщения в почте *gmail.com* (пункт меню «Показать оригинал»)

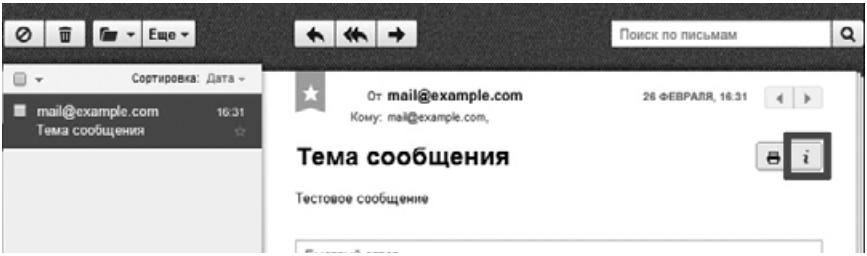


Рис. 5. Поиск служебных заголовков сообщения в почте Рамблер (кнопка «*i*» в правом верхнем углу)

[1] Просмотр служебных заголовков писем // RU-CENTER : сайт. URL: https://www.nic.ru/help/prosmotr-sluzhebnyh-zagolovkov-pisem_6806.html (дата обращения: 15.07.2023); Exchange Online for Office 365 // MXToolBox : сайт. URL: https://mxtoolbox.com/Public/Content/EmailHeaders/ (дата обращения: 15.07.2023).

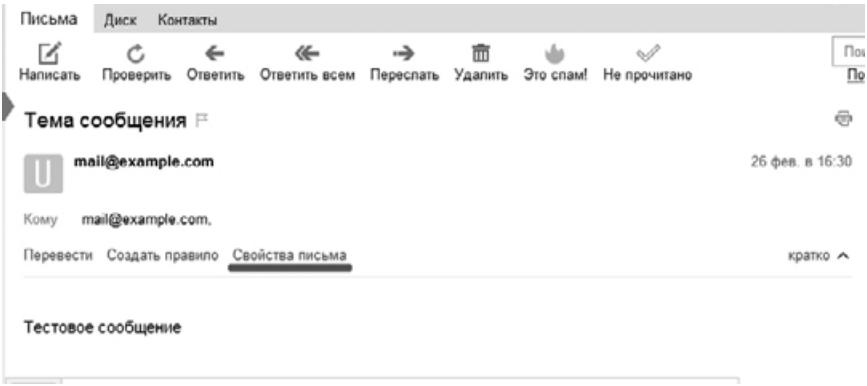


Рис. 6. Поиск служебных заголовков сообщения в Яндекс Почта (кнопка «Свойства письма» на панели инструментов)

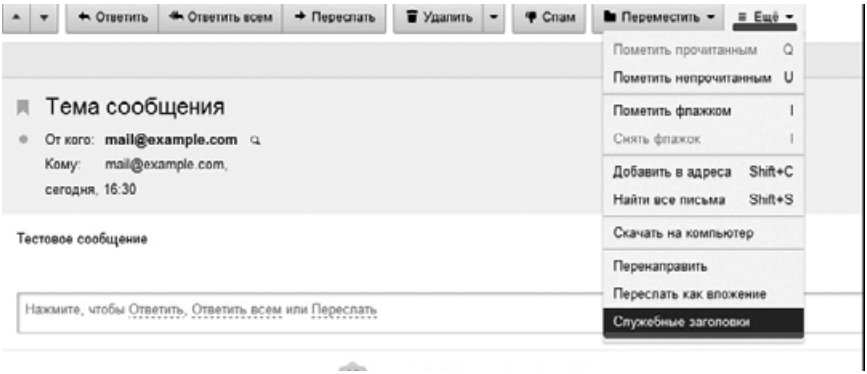


Рис. 7. Поиск служебных заголовков сообщения в почте *mail.ru* (кнопка «Еще» на панели инструментов, далее – «Служебные заголовки»)

Прочитать (интерпретировать) служебные заголовки электронного письма можно в отдельных сервисах:

https://mxtoolbox.com/EmailHeaders.aspx;

https://www.iptrackeronline.com/email-header-analysis.php;

https://mha.azurewebsites.net/;

https://suip.biz/ru/?act=email.

Исследование служебных заголовков письма позволяет интерпретировать историю прохождения электронного письма между почтовыми серверами, что дает возможность отследить почтовый сервис его изначального отправителя.

3. Анализ доменного имени электронного почтового ящика. Доменное имя – символьное имя, служащее для идентификации областей, которые являются единицами административной автономии в сети Интернет, в составе вышестоящей по иерархии такой области. Каждая из таких областей называется доменом. Если это имя не принадлежит одному из общедоступных сервисов, предоставляющих услуги электронной почты (*mail.ru*, *gmail.com* и т. п.), то получение данных о владельце домена может иметь существенное значение для установления личности отправителя электронного письма. Сведения о владельце доменного имени можно получить в одном из сервисов *WHOIS*, например, *https://whois.domaintools.com/*.

Ограничения, установленные законодательством о защите персональных данных, вынудили большинство *WHOIS*-сервисов ограничить выдачу информации о владельцах доменов. Вместе с тем архивную информацию из сервисов *WHOIS* (включая персональные данные владельцев доменов) можно получить в следующих сервисах (рис. 8):

https://drs.whoisxmlapi.com/whois-history;
http://whoishistory.ru/.

Рис. 8. Пример разницы в выдаче данных в сервисах *WHOIS* и в архиве *WHOIS*

4. Получение информации о пользователе сервиса отправки/получения электронных сообщений (контакты, имя (никнейм), аватар, используемые устройства) при помощи средств восстановления доступа. Применительно к наиболее распространенным сервисам электронной почты такими средствами являются:

https://accounts.google.com/ServiceLogin/signinchooser;
https://passport.yandex.ru/auth;
https://account.mail.ru/recovery.

Использование системы восстановления доступа позволяет получить некоторую часть сведений о пользователе (часть телефонного номера или электронной почты, указанные при регистрации, аватар или имя пользователя).

Применительно к отдельным сервисам электронной почты (Яндекс Почта, *Gmail* и др.) существуют программные средства, позволяющие получать частичные пользовательские данные:

https://tools.epieos.com/email.php (для почтовых ящиков *gmail.com*);

https://t.me/UniversalSearchBot (для почтовых ящиков *yandex.ru*).

При этом следует отметить особенность электронной почты *Gmail*: владельцы адресов электронной почты сторонних сервисов при использовании ими устройств с операционной системой *Android* могут получать уникальный идентификатор *Google ID* и, соответственно, раскрывать часть данных о себе в сервисах *Google*.

5. Эффективным способом установления личности владельцев адресов электронной почты является использование специализированных онлайн-сервисов для проверки фактов использования этих адресов в качестве регистрационных данных на различных интернет-порталах и сайтах (социальных сетях, мессенджерах, досках объявлений, резюме и т. д.) (рис. 9). Такими онлайн-сервисами, в частности, являются ТелПоиск, ИнфоСфера, *Pipl*, а также программные продукты *Maltego*, *IBM i2* и др. Эту работу можно проводить и в ручном режиме.

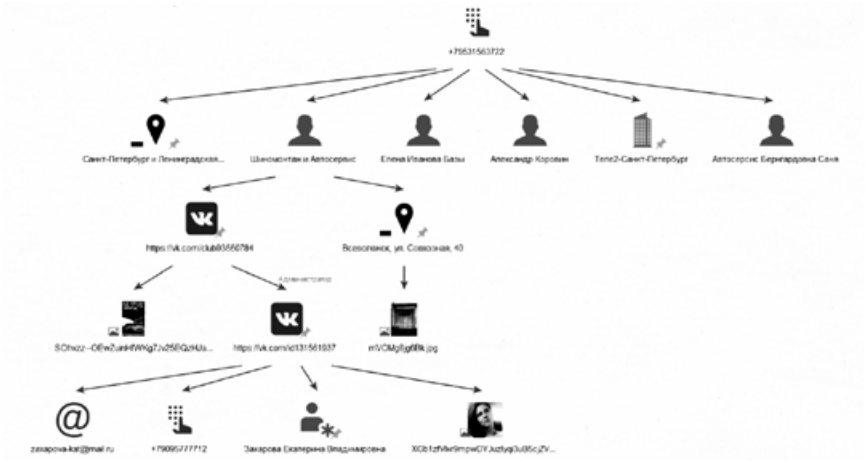


Рис. 9. Представление данных первичной проверки номера телефона в программном комплексе «Охотник» на базе системы визуализации данных *Maltego*

6. Существенный интерес могут представлять сами адреса электронной почты, а также пароли к ним. Поиск паролей по адресу электронной почты можно осуществить в следующих сервисах:

https://leak-lookup.com/;

https://leakpeek.com/;

https://breachdirectory.org/passwords.html;

https://eyeofgod.cc/;

https://leakcheck.io/;

https://github.com/jdiazmx/karma/tree/dd49cace6f68772397a66b04860c10a93f4eb505;

http://xjypo5vzgmo7jca6b322dnqbsdnp3amd24ybx26x5nxbusccjkm4pwid.onion/.

Совпадение паролей, как и совпадение никнеймов, может говорить об использовании различных электронных ящиков одним и тем же лицом.

Проиллюстрируем сказанное на примере адреса электронной почты *yuryevichn@gmail.com*, который был использован для распространения заведомо ложного сообщения об акте терроризма в сентябре 2020 г. (рис. 10).

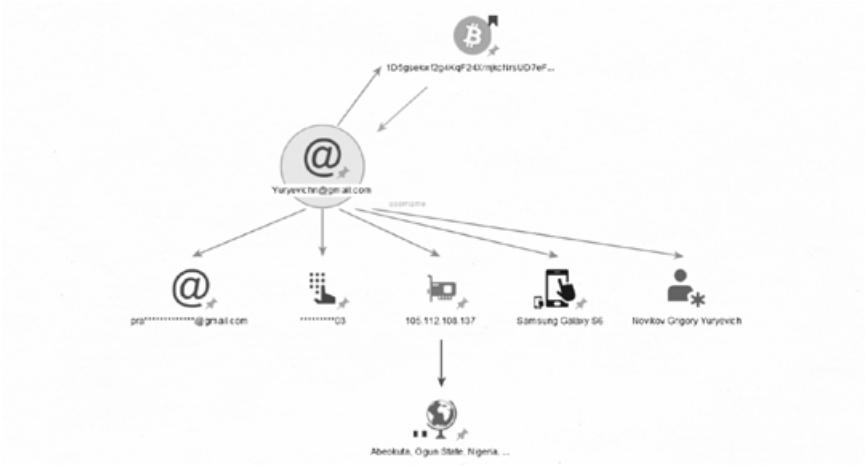


Рис. 10. Представление данных первичной проверки адреса электронной почты в программном комплексе «Охотник» на базе системы визуализации данных *Maltego*

SMTP-запрос по данному почтовому ящику показал, что он является фактически существующим. Осмотр служебного заголов-

ка сообщения позволил получить сведения об IP-адресе его отправителя – 105.112.108.137. Однако он оказался анонимизированным, поскольку принадлежит VPN-сервису, использованному злоумышленником для сокрытия своего реального IP-адреса.

Попытка восстановления доступа к адресу электронной почты на сервисе *https://accounts.google.com/ServiceLogin/signinchooser* позволила установить устройство, используемое для входа в сервис электронной почты. Им оказался смартфон *Samsung Galaxy S6*. Для восстановления доступа злоумышленником были указаны дополнительные контакты, частично скрытые *Google*. В их числе присутствовали номер телефона *********03 и адрес электронной почты *pra**********@gmail.com*.

Анализ электронной почты в сервисе *https://tools.epieos.com/email.php* позволил установить данные, указанные при ее регистрации, в том числе имя пользователя – *Novikov Grigory Yuryevich*, дату последнего использования почтового ящика и связанные сервисы.

Текст письма злоумышленника содержал требование оплаты выкупа на криптовалютный кошелек, имеющий адрес *1D5gsekwf2g4KqF24XrnjkcNrsUD7eFc2o*, исследование которого позволило обнаружить координацию и оплату работы «минера» на нескольких форумах в Даркнете.

7. Использование ADINT-методики для установления пользователей адресов электронной почты. За последние несколько лет широкое распространение получила таргетированная реклама, в которой используются методы поиска целевой аудитории, основанные на характеристиках полученных профилей пользователей и иных открытых источников. С развитием нейросетей, а также увеличением объема данных, генерируемых пользователями электронных устройств, таргетированная реклама становится все более точной. Методика ADINT (от англ. *advertising intelligence* – рекламная разведка) позволяет получать портрет пользователя (пол, возраст, город проживания, интересы и т. п.) и построить на основе этих данных социальный граф, связав его с личным рекламным идентификатором.

Понятие ADINT было введено в конце 2017 г. исследователями Вашингтонского университета[1], которыми в ходе практического эксперимента была доказана возможность использовать целевую

[1] ADINT: Using Targeted Advertising for Personal Surveillance // Paul G. Allen School of Computer Science & Engineering, University of Washington : сайт. URL: https://adint.cs.washington.edu/ (дата обращения: 16.07.2023).

рекламную систему для наблюдения за объектами на основе применения уникальных рекламных идентификаторов пользователей, получаемых из информационных ресурсов, привязанных к номеру мобильного телефона, адресу электронной почты или MAC-адресу электронного устройства пользователя.

Ключевой особенностью ADINT является возможность отслеживать перемещения пользователей по всему миру, используя для этого опции геотаргетированной рекламы.

«Склейка» пользовательских данных в единый граф осуществляется в процессе использования различных цифровых устройств, авторизованных в одном аккаунте, а также при авторизации в ином аккаунте в процессе использования уже известного системе устройства. Иными словами, IT-компании могут продолжать отслеживать фактическое устройство пользователя по его уникальному рекламному идентификатору даже в том случае, если человек сменил адрес электронной почты, номер мобильного телефона или даже сам гаджет.

Узнать о наличии рекламного идентификатора по адресу электронной почты можно несколькими способами.

Для установления Яндекс ID необходимо перейти в Яндекс Коллекции по ссылке *yandex.ru/collections/user/имя* Яндекс Почты. Затем, кликнув на странице правой кнопкой мыши, следует выбрать «Просмотр кода страницы», после чего, используя функцию поиска, находим «cover_info», перед которым будет пользовательский Яндекс ID[1].

Уже сам факт выявления уникального рекламного Яндекс ID позволяет обратиться в компанию Яндекс за получением выгрузки полных данных пользователя, использующего данный идентификатор. Схожим путем осуществляется работа и с иными рекламными площадками: *https://ads.google.com/*, *https://target.my.com/* и др.

Кроме того, можно отслеживать перемещения пользователя по его рекламному идентификатору. Для этого необходимо запустить рекламную кампанию по заданному списку пользовательских идентификаторов (телефон, почта или MAC-адрес), определив целевую аудиторию, которой будет выводиться та или иная реклама, и указав конкретные географические зоны, в которых эта реклама будет показываться. Как только пользователь, имеющий соответствующий рекламный идентификатор, окажется в задан-

[1] Идентификаторы пользователей Google и Яндекс для слежки // SecurityLab.ru : сайт. URL: https://www.securitylab.ru/blog/company/CABIS/348481.php (дата обращения: 16.07.2023).

ной географической зоне, он получит рекламное уведомление, а «рекламодатель», в свою очередь, получит уведомление о том, что один из исследуемых пользователей посетил заданную географическую зону и получил в ней рекламное сообщение.

Стоит отметить, что точность установления геолокационных данных пользователя зависит от таких параметров, как включение на устройстве пользователя модулей связи (GPS, LBS, Wi-Fi), а также от радиуса заданной географической зоны. Наибольшую точность ADINT показывает при осуществлении рекламной рассылки через мобильные приложения.

Особенности установления лиц, использующих телефонную связь для направления заведомо ложных сообщений об актах терроризма.

Методы и средства установления лиц, направивших заведомо ложные сообщения об актах терроризма с использованием абонентских номеров телефонной связи, схожи с рассмотренными выше методами установления лиц, использующих для направления заведомо ложных сообщений об актах терроризма сервисы электронной почты. При этом требуется решение следующих задач:

1. Установление фактического существования абонентского номера, зафиксированного при получении сообщения, а также его принадлежности к номерной емкости конкретного оператора связи. Эта задача решается при помощи запросов к исследуемому номеру мобильного телефона, создаваемых посредством специализированных сервисов, например *https://smsc.ru/* [1].

2. Проверка личности вероятного владельца абонентского номера с использованием онлайн-сервисов определения входящих звонков с неизвестных номеров. Такие приложения используются для определения личности звонящего с абонентского номера, не внесенного в телефонную книгу абонентского устройства пользователя. При этом определяется имя звонящего, его местонахождение, выдается предупреждение в случае совершения нежелательного вызова (спам, мошенничество и т. п.). К подобного рода сервисам относятся:

https://getcontact.com/;
https://sync.me/;
https://www.truecaller.com/;
https://www.kaspersky.ru/caller-id;

[1] Проверка номера мобильного телефона осуществляется путем отправки невидимого смс-сообщения.

https://yandex.ru/promo/alice/callerid.

3. Использование онлайн-сервисов дистанционного банковского обслуживания для установления принадлежности абонентского номера. В частности, одним из таких сервисов является мобильное приложение или онлайн-сервис СберБанк Онлайн, расположенный по ссылке *https://online.sberbank.ru/CSAFront/index.do#/*. Он позволяет определить часть имени пользователя (имя, отчество и первую букву фамилии) при попытке осуществить ему перевод денежных средств по номеру мобильного телефона.

4. Использование Telegram-ботов для поиска информации по абонентскому номеру мобильного телефона. Telegram-боты представляют собой специальные программы-роботы, позволяющие автоматизировать процессы поиска информации. Доступ к большинству из них является платным, однако в большинстве случаев разработчиками предусматривается возможность выполнения некоторого числа бесплатных запросов в целях проверки функциональных возможностей бота. При этом следует иметь в виду, что достоверность, актуальность и полнота получаемой с их использованием информации находятся на весьма низком уровне. Для выполнения поиска информации о владельце абонентского номера могут применяться следующие Telegram-боты:

https://t.me/Tpoisk_Bot;
https://t.me/getfb_bot;
https://t.me/UniversalSearchBot;
https://avclick.me/v/AVinfoBot.

В большинстве случаев при распространении заведомо ложных сообщений об актах терроризма используются средства виртуальной телефонии (*Voice over Internet Protocol* – VoIP) с функцией подмены телефонного номера. Виртуальная телефония обеспечивает голосовую связь по интернет-протоколу IP, выполняя функции набора номера, дозвона и двустороннего голосового общения. От обычной мобильной связи она отличается тем, что для ее использования не требуется самого телефонного аппарата (оконечного оборудования) и идентификационного модуля (симкарты), а также подключения к базовой станции подвижной связи. Соединение устанавливается через специальное приложение по протоколу IP. При применении анонимайзеров установление реального IP-адреса, использованного для соединения, носит затруднительный характер.

Организация подмены телефонного номера осуществляется по примерной схеме, изображенной на рис. 11.

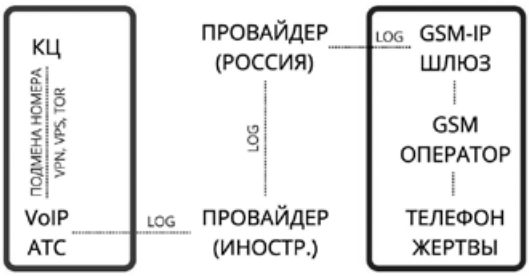


Рис. 11. Примерная схема осуществления подмены телефонного номера звонящего абонента

На начальном этапе приобретаются услуги виртуального колл-центра (программного или аппаратного), включающего возможность подмены абонентского номера телефона. В настоящее время на рынке услуг связи существует значительное число предложений по организации подмены номера, местоположения и изменения голоса при исходящем вызове. Поток данных, идущий из такого колл-центра, поступает иностранному провайдеру, предоставляющему услуги передачи данных. Затем этот иностранный провайдер передает трафик российскому глобальному провайдеру (чаще всего им оказывается Ростелеком), который в соответствии со ст. 10.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» обязан хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, а также саму передаваемую информацию. Далее российский провайдер перенаправляет трафик в шлюз IP-GSM оператора сотовой связи, который задействует собственную сеть GSM для связи с конечным абонентом (потерпевшим).

Согласно п. 9 ст. 46 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[1] оператор связи, с сети передачи данных которого инициируется соединение для целей передачи голосовой информации, обязан передавать в сеть передачи данных другого оператора связи, участвующего в установлении соединения, в неизменном виде уникальный код идентификации, выделенный на основании договора об оказании услуг связи абоненту, инициировавшему соединение для

[1] О связи : Федер. закон № 126-ФЗ : принят Гос. Думой 18 июня 2003 г. : одобрен Советом Федерации 25 июня 2003 г. : в ред. от 4 авг. 2023 г. // СПС КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 06.08.2023).

целей передачи голосовой информации. Однако на практике данное требование распространяется только на российских операторов связи, чем активно пользуются организаторы анонимных соединений.

Следует также отметить, что Федеральным законом от 2 июля 2021 г. № 319-ФЗ «О внесении изменений в Федеральный закон "О связи"»[1] установлено, что при оказании услуг связи и (или) услуг по пропуску трафика оператор связи обязан проверить соблюдение вышеназванных требований и прекратить оказание услуг связи и (или) услуг по пропуску трафика в свою сеть связи в случае:

– если установлено отсутствие информации об инициировании соединения абонентом (за исключением случая, если соединение инициировано с сети связи иностранного оператора связи и сопровождается нумерацией, соответствующей иностранной системе и плану нумерации);

– если инициированное с сети связи иностранного оператора связи соединение сопровождается нумерацией, соответствующей российской системе и плану нумерации;

– если у оператора связи, участвующего в установлении соединения, в том числе для передачи короткого текстового сообщения, отсутствует информация об абонентском номере или уникальном коде идентификации абонента, инициировавшего это соединение.

Данные изменения вступили в силу с 1 января 2023 г. Представляется, что приведенные положения воспрепятствуют криминальному использованию технологий подмены абонентских номеров. В целях противодействия использованию подмены телефонных номеров в криминальных целях российский интернет-провайдер должен передавать оператору связи в неизменном виде данные иностранного провайдера VoIP (наименование провайдера, дату и время соединения, IP-адрес сервера). Оператор подвижной связи сможет маркировать входящий звонок своим абонентам как VoIP, а не GSM, учитывая это в скоринговой оценке звонка и выделяя иностранных провайдеров, которые чаще всего используются при осуществлении противоправной деятельности.

Программные продукты, предназначенные для идентификации пользователей адресов электронной почты и номеров телефонов. Комплексное применение методов, рассмотренных выше, может осуществляться с использованием программных средств, использующих данные из различных источников происхождения (поисковые сервисы, социальные сети, доски объявлений и резюме,

[1] О внесении изменений в Федеральный закон «О связи» : Федер. закон № 319-ФЗ : принят Гос. Думой 17 июня 2021 г. : одобрен Советом Федерации 23 июня 2021 г. // Собр. законодательства Рос. Федерации. 2021. № 27 (ч. 1). Ст. 5147.

мессенджеры, даркнет, данные геоинформационных систем, открытые данные государственных органов). К ним относятся:

https://интернет-розыск.рф/telpoisk;

https://инфосфера.рус/ и др.

Для одновременной проверки большого числа идентификаторов предназначен программный комплекс «Охотник» (№ 13316 от 15 апреля 2022 г. в реестре российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации, свидетельство о государственной регистрации программы для ЭВМ № 2021680077 от 7 декабря 2021 г., разработчик – ООО «Ти Хантер», ИНН 7810739096, сайт *https://tomhunter.ru/analiticheskaya-platforma-ohotnik*). Комплекс осуществляет поиск и анализ информации в социальных сетях, мессенджерах, сегменте сети *Tor* и других открытых источниках (всего более 300) и визуализирует их на одном рабочем месте.

Исследование заведомо ложных сообщений об актах терроризма, отправленных посредством мессенджеров.

Данные, позволяющие установить пользователей мессенджеров, как правило, весьма ограничены и могут включать в себя: фотографию (аватар) пользователя, его имя или никнейм (псевдоним), а также номер мобильного телефона или адрес электронной почты, через которые происходила регистрация аккаунта. Отметим, что имя, никнейм и фотография пользователя являются изменяемыми параметрами.

Вопросы исследования номера мобильного телефона и адреса электронной почты были рассмотрены выше.

Поиск совпадений лиц и объектов по фотографии пользователя мессенджера может осуществляться с использованием следующих сервисов:

https://search4faces.com/;

https://findclone.ru/;

https://yandex.ru/images/.

В поиске совпадений никнейма (псевдонима) пользователя мессенджера с учетными записями в иных программных продуктах могут помочь нижеприведенные сервисы:

https://github.com/soxoj/maigret;

https://github.com/sherlock-project/sherlock;

https://whatsmyname.app/;

https://namecheckup.com/.

Для комплексного поиска учетных записей в социальных сетях по имени, фамилии, возрасту и населенному пункту может использоваться сервис *https://go.mail.ru/search_social.*

При установлении личности пользователей популярного мессенджера Telegram существуют определенные особенности.

Установление уникального неизменяемого идентификационного номера пользователя Telegram возможно посредством использования сервисов:

https://t.me/userinfobot;

https://t.me/CheckID_AIDbot;

https://t.me/username_to_id_bot.

Участие пользователя Telegram в сообществах (чатах) можно выявить при помощи сервисов:

https://t.me/telesint_bot;

https://t.me/tgscanrobot.

Поиск пользователей Telegram по данным геолокации (при выключенных дополнительных настройках конфиденциальности) можно осуществить при использовании сервисов:

https://t.me/locatortlrm_bot;

https://github.com/tejado/telegram-nearby-map.

Установление номера мобильного телефона пользователя Telegram, который по умолчанию скрыт, возможно посредством следующих сервисов:

https://t.me/TgAnalyst_bot:

https://t.me/anonimov_bot.

Кроме этого, идентификация телефонов пользователей мессенджера и иной информации о них возможна в специализированных программных продуктах: «Телеграм-Деанонимайзер» (рис. 12), «Telegram-Insider» и программном комплексе «Охотник».

Рис. 12. Представление данных пользователей Telegram в сервисе «Телеграм-Деанонимайзер»

Указанные системы представляют собой различные агрегаторы данных, полученные из открытых источников. При этом «Telegram-Insider» и «Охотник» включают в себя данные соотнесения номерной емкости сотовых операторов с пользовательскими аккаунтами в Telegram. Сервис «Телеграм-Деанонимайзер» использует сеть специализированных ботов, которые позволяют ему устанавливать не только номера мобильных телефонов, привязанных к мессенджеру, но и получать данные о соединении пользователя, его устройстве и геолокации.

Исследование заведомо ложных сообщений об актах терроризма, отправленных посредством социальных сетей.

Работа по установлению принадлежности учетных записей пользователей социальных сетей имеет сходство с исследованием аккаунтов в мессенджерах.

Принимая во внимание, что социальные сети в юридическом смысле являются организаторами распространения информации, то приведенные выше положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» относительно идентификации личности пользователей, хранения контента и информации о фактах его передачи в полном объеме распространятся и на данные информационные сервисы. Однако не во всех случаях сведения, которыми располагают организации, осуществляющие администрирование социальных сетей, являются актуальными и достоверными. Причины подобного положения также были рассмотрены выше.

В этих условиях применяются методы и средства OSINT, направленные на идентификацию пользователей социальных сетей по размещенным ими фотографиям, именам, датам рождения или никнеймам (псевдонимам). Большое внимание уделяется установлению адреса электронной почты или номера мобильного телефона, использовавшегося для регистрации учетной записи пользователя, а также получению сведений о соединении и устройстве пользователя.

Особенностью социальных сетей является возможность проводить глубокий анализ информации, содержащейся в учетных записях, включая изменение архивной информации профиля, семантический анализ текстов и высказываний, сбор публичных сообщений и переписок пользователя, изучение его круга друзей. Инструментарий для исследования социальных профилей и сообществ в популярной российской социальной сети «ВКонтакте» следующий:

https://220vk.com/;
http://vk.city4me.com/;
https://analyze24.ru/;
https://byratino.info/.

Социальные сети YouTube, «ВКонтакте», Twitter, Instagram, FourSquare, Flickr, Facebook, SnapChat и мессенджер Telegram позволяют выявлять контент пользователей, размещаемый в определенное время и в определенной географической зоне. Сбор и обработка информации пользователей, размещенной ими с указанием данных геолокации, а также установление геолокации по публикуемым фотографиям могут быть произведены при помощи следующего инструментария:

https://mattw.io/youtube-geofind/location;
https://montage.meedan.com/welcome;
https://app.skylens.io/;
https://vk.com/feed?section=search;
http://photo-map.ru/;
http://snradar.azurewebsites.net/;
https://twitter.com/search-advanced;
https://github.com/TIGMINT/TIGMINT;
https://onemilliontweetmap.com/;
https://twimap.com/;
https://github.com/coldfusion39/geOSINT;
https://www.osintcombine.com/instagram-explorer;
https://www.instagram.com/explore/locations/;
https://instmap.com/;
https://whopostedwhat.com/;
https://map.snapchat.com/;
https://t.me/locatortlrm_bot;
https://github.com/tejado/telegram-nearby-map.

Сервис *https://github.com/instaloader/instaloader* предназначен для выгрузки всего пользовательского контента, включая фотографии, видеофайлы, тексты, описания и теги.

В соответствии со ст. 10.6 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» владелец социальной сети обязан не допускать ее использования для совершения противоправных действий, а также осуществлять мониторинг размещаемой в ней информации в целях выявления недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи. В слу-

чае выявления подобной информации владелец социальной сети обязан незамедлительно принять меры по ограничению доступа к ней.

Исследование криптовалютных кошельков, используемых для получения выкупа при отправлении заведомо ложных сообщений об актах терроризма.

В большинстве случаев для получения финансовых средств от своих жертв злоумышленниками используются криптовалютные кошельки.

С юридической точки зрения криптовалюту можно определить как имущество в электронной форме, созданное с использованием криптографических средств и учитываемое в распределенном реестре цифровых транзакций в соответствии с установленными правилами его ведения.

Ч. 3 ст. 1 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[1] дает легальное определение цифровой валюты, под которой понимается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам.

При этом согласно ч. 5 ст. 14 вышеуказанного Федерального закона налоговым резидентам Российской Федерации запрещается принимать цифровую валюту в качестве встречного предоставления за передаваемые ими (им) товары, выполняемые ими (им) работы, оказываемые ими (им) услуги или иного способа, позволяющего предполагать оплату цифровой валютой товаров (работ, услуг). А в соответствии с ч. 7 цитируемой статьи в Российской Федерации запрещается распространение информации о предложении и (или)

[1] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федер. закон № 259-ФЗ : принят Гос. Думой 22 июля 2020 г. : одобрен Советом Федерации 24 июля 2020 г. : в ред. от 14 июля 2022 г. // СПС КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 06.08.2023).

приеме цифровой валюты в качестве встречного предоставления за передаваемые ими (им) товары, выполняемые ими (им) работы, оказываемые ими (им) услуги или иного способа, позволяющего предполагать оплату цифровой валютой товаров (работ, услуг).

С технической точки зрения криптовалюта представляет собой распределенную основанную на математических принципах пиринговую виртуальную валюту с открытым исходным кодом, при использовании которой отсутствует централизованный администратор, а также соответствующие контроль и надзор со стороны государственных органов или иных третьих лиц. На апрель 2021 г. число криптовалют превышало 4 800 (2 541 из которых было зарегистрировано и торговалось на криптобиржах). Наибольшей капитализацией из криптовалют обладают Bitcoin (удерживающий до 56 % рынка), Ethereum, XRP, Bitcoin Cash, Litecoin и Stellar.

Криптовалюты имеют существенные отличия от привычных финансовых транзакций, совершаемых при помощи банковских счетов, карт или централизованных электронных денег.

Во-первых, для функционирования криптовалюты не требуется централизованный регулятор или эмитент. При этом все транзакции криптовалюты публичны и отражаются в реестре данных операций, формируемом на основе технологии блокчейна.

Во-вторых, владельцы криптовалюты считаются анонимными за счет того, что каждая транзакция подлежит регистрации с присвоением уникального номера, однако эта регистрация привязывается к электронному кошельку, а не к личности его владельца. При этом сам криптокошелек может быть открыт на вымышленных лиц. На практике это означает, что в публичном блокчейне полностью отсутствуют данные о фактическом владельце того или иного криптовалютного кошелька.

Криптокошелек – это эквивалент банковского счета, на котором пользователи хранят свою криптовалюту и совершают транзакции. Существующие криптокошельки можно разделить на следующие типы: аппаратные, программные и онлайн-кошельки. Критерием отнесения кошельков является место хранения приватного ключа, являющегося основным средством соотнесения криптокошелька с конкретным пользователем. Кроме того, пользователь имеет фактически неограниченную возможность создания уникальных адресов (примерный аналог – номер банковского счета) для своего криптовалютного кошелька.

В-третьих, осуществление транзакций криптовалюты осуществляется не напрямую, а путем смешения групп транзакций в блоки (отсюда и название «блокчейн» – от англ. «цепь из блоков»). Блок транзакций – специальная структура для записи группы транзакций в блокчейн. Эта особенность позволяет подтверждать и перепрове-

рять совершенные транзакции, делая криптовалютные операции прозрачными для любого пользователя. Любой интернет-пользователь имеет возможность свободно просмотреть и исследовать блокчейн в таких обозревателях, как *btc.com*, *etherscan.io*, *localmonero.co* и др.

В-четвертых, криптовалюты являются как средством взаиморасчетов, так и объектом инвестирования. В этой связи криминальные взаиморасчеты с использованием криптовалют не всегда завершаются выводом средств в фиатные валюты. Криптовалюта может годами накапливаться в определенном цифровом кошельке, «консервируя» преступный доход.

По своей сути криптовалюта на основе блокчейна представляет собой цепочку цифровых подписей, отражающих путь денежных средств в системе. Конечная цель механизма транзакций заключается в том, чтобы любой узел системы мог узнать подробности осуществленной сделки, отображенные в транзакции. Это достигается путем осуществления подписи и проверки некоторых элементов транзакции с использованием схем электронной подписи. Таким образом участники системы могут легко отслеживать пути перемещения средств в системе, а также контролировать целостность сервиса.

Согласно рекомендациям Группы разработки финансовых мер по борьбе с отмыванием денег (ФАТФ), организация обращения цифровой валюты строится на основе принципа «знай своего клиента» (KYC). В соответствии с требованиями этого принципа организация, осуществляющая деятельность по выпуску или обращению цифровой валюты, обязана идентифицировать и верифицировать личность каждого клиента. Причем сделать это нужно прежде, чем он сможет проводить финансовые операции.

Криптообменные биржи располагают как минимум следующей информацией о зарегистрированных на них клиентах: ФИО, дате рождения, электронной почте, номере телефона, стране и адресе проживания, документе, удостоверяющем личность.

Кроме того, криптообменные биржи располагают данными о проведенных их клиентами операциях: статусе обменной операции (выполнено/закрыта); сумме ввода (сумма обмена в Bitcoin) и вывода (сумма, полученная в рублях в результате обменной операции), номерах счетов получателя, дате и времени создания, изменения.

Всего в русскоязычном домене сети Интернет (по данным мониторинга *bestchange.ru*) представлено более 400 интернет-площадок по обмену криптовалют на их рублевый эквивалент, которые находятся вне поля правового регулирования.

Существующая методология деанонимизации транзакций криптовалюты предполагает необходимость отслеживания всей

цепочки их совершения – от момента проведения криминального платежа и до предполагаемого обналичивания (обмена) криптовалюты на фиатные деньги. Последние представляют собой не обеспеченные золотом и другими драгоценными металлами деньги, номинальная стоимость которых устанавливается и гарантируется государством вне зависимости от стоимости материала, использованного для их изготовления, на криптовалютной бирже, в обменнике или банкомате, терминале самообслуживания.

Для сбора данных о криптокошельках и отслеживания их транзакций можно использовать как штатные, так и универсальные обозреватели блокчейна, позволяющие анализировать транзакции нескольких видов криптовалют. К числу последних следует отнести:

https://blockchair.com/;
https://tokenview.com/;
https://live.blockcypher.com/.

Анализ и сопоставление данных блокчейна в текстовом виде крайне затруднены в связи с объемом информации. Поэтому для визуального представления и исследования криптовалютных транзакций (рис. 13) предлагается использовать ряд бесплатных или условно бесплатных решений, таких как:

https://blockpath.com/;
https://oxt.me/;
https://graphsense.info/;
https://github.com/s0md3v/Orbit;
http://sicp.ueba.su/;
https://explorer.crystalblockchain.com/;
https://www.maltego.com/.

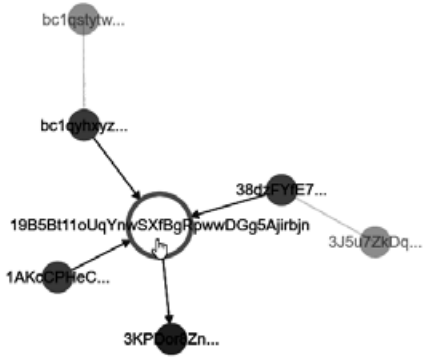


Рис. 13. Представление цепочек транзакций криптовалюты Bitcoin в сервисе *https://blockpath.com/*

Для идентификации криптовалютных кошельков, входящих в исследуемые цепочки транзакций, предлагается использовать следующие источники, имеющие собственные накопленные реестры идентифицированных или соотнесенных с теми или иными сущностями криптокошельков (рис. 14):

https://oxt.me/ (Bitcoin);
http://sicp.ueba.su/ (Bitcoin);
https://explorer.crystalblockchain.com/ (Bitcoin);
https://www.walletexplorer.com/ (Bitcoin);
https://bitinfocharts.com/ (Bitcoin);
https://ethtective.com/ (Ethereum).

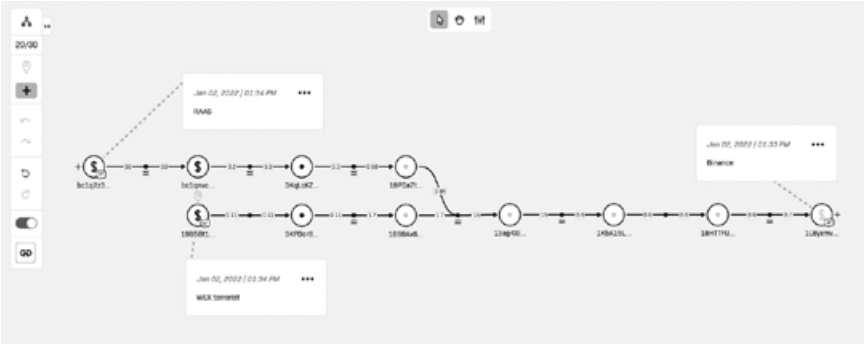


Рис. 14. Представление цепочек транзакций криптовалюты Bitcoin в сервисе *https://crystalblockchain.com/*

Для выявления случаев использования криптовалютных кошельков в противоправных целях (мошенничество, распространение запрещенного контента или вредоносного программного обеспечения, вымогательство, торговля наркотиками) предлагается использовать следующие сайты-отзовики:

https://www.bitcoinabuse.com/;
https://bitcoinwhoswho.com/;
https://checkbitcoinaddress.com/;
https://scam-alert.io/;
https://cryptscam.com/.

К числу иных приемов установления принадлежности криптовалютных кошельков следует отнести использование *Google Dorks* (язык специализированных запросов к поисковой системе *Google*) (рис. 15):

– *[адрес_криптокошелька -block]*, или *[адрес_криптокошелька -explorer]* – позволяет исключить из поисковой выдачи упоминание

отдельного слова. В приведенном примере из поиска будет исключено большинство обозревателей блокчейна;

– *[site:bitcointalk.org адрес_криптокошелька]* – позволяет осуществлять поиск данных о криптокошельке на конкретном сайте. В приведенном примере – на сайте *bitcointalk.org*;

– *[site:https://docs.google.com/spreadsheets Bounty intext:»@gmail.com»]* – позволяет осуществлять поиск таблиц *Google Docs*. В приведенном примере – таблиц, включающих списки идентифицированных криптокошельков в рамках корпоративных программ Bug Bounty.

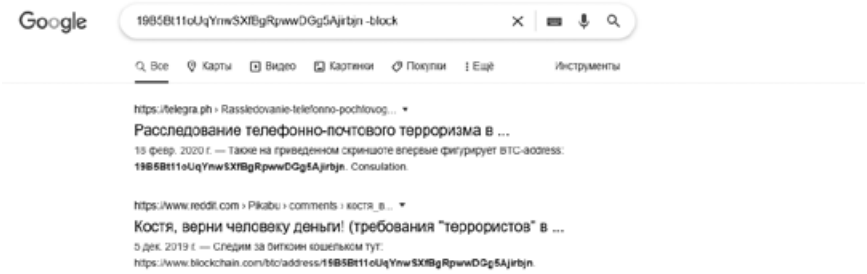


Рис. 15. Пример использования *Google Dorks* для поиска информации о криптокошельке

В целях анонимизации транзакций в криптовалюте используются анонимайзеры, подменяющие IP-адрес устройства, с которого производился вход в сеть Интернет, а также программы-«миксеры», осуществляющие разбиение пересылаемого сообщения на отдельные фрагменты, направляемые адресату разными маршрутами. Большинство «Bitcoin-миксеров» использует следующую технологию: средства клиента дробятся на мелкие части, после чего эти части смешиваются в случайном порядке с частями других клиентов. В результате всех операций к конечному получателю приходит заданное количество криптовалюты, но небольшими партиями от разных случайно выбранных участников. На выходе получается «чистая» криптовалюта, которая переводится владельцу.

Однако на практике отслеживать «миксеры» не так сложно. Для этого необходимо лишь получить информацию о большей части криптокошельков, принадлежащих такому «миксеру». Это достигается путем использования специализированными сервисами по отслеживанию криптовалют аналитических и статистических методов работы. Затем посредством сравнения входных и выходных сумм устанавливается предполагаемый кошелек получателя криптовалюты.

Кроме этого, «миксеры» обладают еще одним существенным недостатком. Криптокошельки, входящие в «миксер», очень быстро становятся непригодными для использования. Дело в том, что крупнейшие сервисы по отслеживанию криптовалют моментально маркируют как неблагонадежные те криптокошельки «миксера», по которым проходили средства, добытые преступным путем.

Наиболее конфиденциальными для совершения транзакций считаются «анонимные криптовалюты». Блокчейны анонимных криптовалют изначально частично или полностью скрывают данные транзакций (адреса отправителя и получателя, сумму сделки и др.). К числу популярных анонимных криптовалют относят: Dash, Monero, Zcash. К менее известным – SmartCash, Komodo, Pivx, Navcoin, Horizen и Verge. Недостаток анонимных криптовалют – низкая ликвидность и слабое принятие вне криптовалютного сообщества и бирж. Иными словами, отследить транзакции анонимной криптовалюты сложно. Но для перевода денег в более ликвидную криптовалюту или в фиатные деньги анонимную криптовалюту придется заводить в одну из известных бирж или обменников, работающих в соответствии с принципом KYC, рекомендациями ФАТФ.

Реально анонимной криптовалютой в криминальном мире считается лишь Monero. Остальные «анонимные криптовалюты» проводят до 70 % транзакций в открытом блокчейне. Разработки электронно-аналитических систем, предназначенных для отслеживания анонимных криптовалют, начались в США в 2018 г. Один из первых таких инструментов был разработан в августе 2020 г. по заказу Министерства внутренней безопасности США американской компанией *CipherTrace*.

Вопросы для самоконтроля

1. Опишите приемы деанонимизации отправителей сообщений электронной почты.
2. Опишите приемы деанонимизации отправителей сообщений, направленных посредством телефонной связи и интернет-телефонии.
3. Опишите приемы деанонимизации отправителей сообщений, направленных посредством сервиса отправки мгновенных сообщений (мессенджеров) и социальных сетей.
4. Опишите приемы деанонимизации владельцев криптовалютных кошельков.

Заключение

Начало специальной военной операции на Украине спровоцировало новую волну ложных сообщений об актах терроризма, распространяемых посредством рассылки через электронную почту *gmail.ru*, регистрируемую автоматически при помощи программного обеспечения. Рассылаемые сообщения заносились в график отправок на будущее, а сами преступники даже не заходили на электронный ящик для его регистрации. При таких обстоятельствах получение данных отправителей у правообладателя сервиса электронной почты не дает ожидаемого результата, удается установить лишь дополнительный адрес электронной почты, который использовался для восстановления доступа, что значительно затрудняет расследование преступлений, предусмотренных ст. 207 Уголовного кодекса Российской Федерации.

В этих условиях перспективным видится создание сервиса автоматизированной верификации почтового ящика отправителя, включая исследование служебных заголовков, проверку его фактического существования и использования для регистрации в онлайн-сервисах, а также установление сведений о соединении и устройстве пользователя почтового ящика.

Список рекомендованной литературы

Нормативные правовые акты

О противодействии терроризму : Федер. закон № 35-ФЗ : принят Гос. Думой 26 февр. 2006 г. : одобрен Советом Федерации 1 марта 2006 г.

О внесении изменений в статью 207 Уголовного кодекса Российской Федерации и статьи 150 и 151 Уголовно-процессуального кодекса Российской Федерации : Федер. закон № 98-ФЗ : принят Гос. Думой 15 апр. 2014 г. : одобрен Советом Федерации 29 апр. 2014 г.

О внесении изменений в статьи 205 и 207 Уголовного кодекса Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации : Федер. закон № 501-ФЗ : принят Гос. Думой 20 дек. 2017 г. : одобрен Советом Федерации 26 дек. 2017 г.

Военная доктрина Российской Федерации : утв. Президентом Рос. Федерации от 25 дек. 2014 г. № Пр-2976.

О Стратегии национальной безопасности Российской Федерации : Указ Президента Рос. Федерации от 2 июля 2021 г. № 400.

Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями : постановление Правительства Рос. Федерации от 20 окт. 2021 г. № 1801.

Об утверждении Инструкции об организации рассмотрения обращений граждан Российской Федерации в органах федеральной службы безопасности : приказ ФСБ России от 30 авг. 2013 г. № 463.

Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях : приказ МВД России от 29 авг. 2014 г. № 736.

Материалы судебной практики

О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности : постановление Пленума Верховного Суда Рос. Федерации от 9 февр. 2012 г. № 1.

О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий : постановление Пленума Верховного Суда Рос. Федерации от 16 окт. 2009 г. № 19.

О судебной практике по уголовным делам о хулиганстве и иных преступлениях, совершенных из хулиганских побуждений : постановление Пленума Верховного Суда Рос. Федерации от 15 нояб. 2007 г. № 45.

О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда Рос. Федерации от 27 дек. 2002 г. № 29.

О судебной практике по делам об убийстве (ст. 105 УК РФ) : постановление Пленума Верховного Суда Рос. Федерации от 27 янв. 1999 г. № 1.

Научная и учебная литература

Бриллиантов, А. Заведомо ложный донос: вопросы квалификации // Уголовное право. – 2014. – № 3. – С. 22–26.

Важенин, С. Г. Социальная инфраструктура народнохозяйственного комплекса. – Москва : Наука, 1984. – 170 с.

Гаврилин, Ю. В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : науч.-практ. пособие. – Москва : Академия управления МВД России, 2021. – 72 с.

Гаврилин, Ю. В. Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств : учеб. пособие / Ю. В. Гаврилин, И. С. Бедеров. – Москва : Академия управления МВД России, 2022. – 76 с.

Гаврилин, Ю. В. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : учеб. пособие / Ю. В. Гаврилин, Г. З. Гаспарян. – Москва : Проспект, 2021. – 128 с.

Гаухман, Л. Д. Ответственность за преступления против собственности / Л. Д. Гаухман, С. В. Максимов. – 2-е изд., испр. – Москва : АО «Центр ЮрИнфоР», 2001. – 310 с.

Емельянов, В. Террористический акт и акт терроризма: понятие, соотношение и разграничение // Законность. – 2002. – № 7. – С. 44–46.

Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учеб. пособие / А. А. Балашова, В. Ф. Васюков, Ю. В. Гаврилин [и др.] ; под ред. Ю. В. Гаврилина и А. В. Победкина. – Москва : Академия управления МВД России, 2021. – 140 с.

Ковлагина, Д. А. Проблемы дифференциации ответственности за заведомо ложное сообщение об акте терроризма // Уголовное право. – 2019. – № 6. – С. 46–50.

Комментарий к Уголовному кодексу Российской Федерации (постатейный) / К. А. Барышева, Ю. В. Грачева, Г. А. Есаков [и др.] ;

под ред. Г. А. Есакова. – 7-е изд., перераб. и доп. – Москва : Проспект, 2017. – 736 с.

Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Г. Н. Борзенков, В. П. Верин, Б. В. Волженкин [и др.] ; отв. ред. В. М. Лебедев. – 7-е изд., перераб. и доп. – Москва : Юрайт-Издат, 2007. – 902 с.

Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. И. Чучаева. – 2-е изд., испр., доп. и перераб. – Москва : КОНТРАКТ, ИНФРА-М, 2010. – 1040 с.

Кригер, Г. А. Проблемы социальной обусловленности уголовного закона / Г. А. Кригер, Н. Ф. Кузнецова. – Москва : Юрид. лит., 1977. – 122 с.

Овчинникова, Г. В. Терроризм / науч. ред. Б. В. Волженкин. – Санкт-Петербург : Санкт-Петербург. юрид. ин-т Генеральной прокуратуры Рос. Федерации, 1998. – 36 с.

Сычева, И. В. Исследование содержания категории «социальная инфраструктура» / И. В. Сычева, Н. А. Сычева // Известия Тульского государственного университета. Экономические и юридические науки. – 2012. – № 2–1. – С. 230–238.

Торопов, Б. А. Моделирование ситуации информационного противодействия деструктивным влияниям в социальных сетях по резонансным общественно-политическим вопросам : моногр. – Москва : Академия управления МВД России, 2022. – 100 с.

Уголовное право. Особенная часть : учеб. для вузов / под ред. И. Я. Козаченко, З. А. Незнамовой, Г. П. Новоселова. – Москва : Норма, 1997. – 768 с.

Уголовное право России. Часть Особенная : учеб. для вузов / отв. ред. Л. Л. Кругликов. – 2-е изд., перераб. и доп. – Москва : БЕК. 2004. – 448 с.

Чернец, В. Влияние через социальные сети / В. Чернец, Т. Базлова, Э. Иванова ; под общ. ред. Е. Г. Алексеевой. – Москва : Фонд «ФОКУС-МЕДИА», 2010. – 200 с.

ДЛЯ ЗАМЕТОК

Учебное издание

Гаврилин Юрий Викторович, **Мартыненко** Наталия Эдуардовна,
Бедеров Игорь Сергеевич

**ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ
ЗАВЕДОМО ЛОЖНЫХ СООБЩЕНИЙ
ОБ АКТАХ ТЕРРОРИЗМА**

Редактор: К.В. Громова
Верстка А.Е. Скрипаковой

Подписано в печать 27.10.2023. Формат 60×84 $^{1}/_{16}$.
Усл. печ. л. 4,42. Уч.-изд. л. 3,44. Тираж 65 экз. Заказ .

Отделение полиграфической и оперативной печати РИО
Академия управления МВД России
125171, Москва, ул. Зои и Александра Космодемьянских, д. 8

ISBN 978-5-907530-85-0