Отчет о проверке

Автор: Таршева Мира Николаевна

Проверяющий: Таршева Мира Николаевна

Название документа: Таршева МН_Вестник ТГУ

Организация: Орловский юридический институт МВД России имени В.В. Лукьянова

РЕЗУЛЬТАТЫ ПРОВЕРКИ

Совпадения:
6,82%

Оригинальность:
65,27%

Цитирования:
27,91%

Самоцитирования:
0%

«Совпадения», «Цитирования», «Самоцитирования», «Оригинальность» являются отдельными показателями, отображаются в процентах и в сумме дают 100%, что соответствует проверенному тексту документа.

- **Совпадения** — фрагменты проверяемого текста, полностью или частично сходные с найденными источниками, за исключением фрагментов, которые система отнесла к цитированию или самоцитированию. Показатель «Совпадения» – это доля фрагментов проверяемого текста, отнесенных к совпадениям, в общем объеме текста.
- **Самоцитирования** — фрагменты проверяемого текста, совпадающие или почти совпадающие с фрагментом текста источника, автором или соавтором которого является автор проверяемого документа. Показатель «Самоцитирования» – это доля фрагментов текста, отнесенных к самоцитированию, в общем объеме текста.
- **Цитирования** — фрагменты проверяемого текста, которые не являются авторскими, но которые система отнесла к корректно оформленным. К цитированиям относятся также шаблонные фразы; библиография; фрагменты текста, найденные модулем поиска «СПС Гарант: нормативно-правовая документация». Показатель «Цитирования» – это доля фрагментов проверяемого текста, отнесенных к цитированию, в общем объеме текста.
- **Текстовое пересечение** — фрагмент текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника.
- **Источник** — документ, проиндексированный в системе и содержащийся в модуле поиска, по которому проводится проверка.
- **Оригинальный текст** — фрагменты проверяемого текста, не обнаруженные ни в одном источнике и не отмеченные ни одним из модулей поиска. Показатель «Оригинальность» – это доля фрагментов проверяемого текста, отнесенных к оригинальному тексту, в общем объеме текста.

Обращаем Ваше внимание, что система находит текстовые совпадения проверяемого документа с проиндексированными в системе источниками. При этом система является вспомогательным инструментом, определение корректности и правомерности совпадений или цитирований, а также авторства текстовых фрагментов проверяемого документа остается в компетенции проверяющего.

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Номер документа: 489

Тип документа: Не указано

Дата проверки: 13.03.2025 15:13:11

Дата корректировки: Нет

Количество страниц: 9

Символов в тексте: 23580

Слов в тексте: 2721

Число предложений: 304

Комментарий: не указано

ПАРАМЕТРЫ ПРОВЕРКИ

Выполнена проверка с учетом редактирования: Да

Исключение элементов документа из проверки: Нет

Выполнено распознавание текста (OCR): Нет

Выполнена проверка с учетом структуры: Нет

Модули поиска: Интернет Плюс, Кольцо вузов, Переводные заимствования издательства Wiley (RuEn), Патенты СССР, РФ, СНГ, Переводные заимствования по Интернету (EnRu), Издательство Wiley, Переводные заимствования (RuEn), eLIBRARY.RU, Цитирование, Перефразирования по Интернету, Шаблонные фразы, СПС ГАРАНТ: нормативно-правовая документация, Библиография, СПС ГАРАНТ: аналитика, ИПС Адилет, Публикации eLIBRARY (переводы и перефразирования), Сводная коллекция РГБ, Диссертации НББ, Сводная коллекция ЭБС, Медицина

ИСТОЧНИКИ

№	Доля в тексте	Доля в отчете	Источник	Актуален на	Модуль поиска	Комментарий
[01]	15,91%	15,91%	не указано	07 Сен 2022	Библиография	
[02]	7,71%	7,71%	не указано	07 Сен 2022	Цитирование	
[03]	4%	0%	Сущенок О.А. Уголовная ответст...	29 Янв 2021	Кольцо вузов	
[04]	4%	0%	Сущенок О.А. Уголовная ответст...	03 Фев 2021	Кольцо вузов	
[05]	3,74%	0%	118610	26 Июн 2021	Кольцо вузов	
[06]	3,69%	0%	Преступления террористическо... http://elibrary.ru	01 Янв 2023	eLIBRARY.RU	
[07]	3,55%	0,68%	ЮНиП № 1 (65) (1)	28 Янв 2025	Сводная коллекция вузов МВД	
[08]	3,46%	0,65%	87709	08 Июн 2021	Кольцо вузов	
[09]	3,38%	0,16%	Ковлагина, Дарья Александровн... http://dlib.rsl.ru	01 Янв 2016	Сводная коллекция РГБ	
[10]	3,37%	0%	Ковлагина, Дарья Александровн... http://dlib.rsl.ru	01 Янв 2016	Сводная коллекция РГБ	
[11]	3,24%	0,13%	Курдуков, Андрей Николаевич Уг... http://dlib.rsl.ru	01 Янв 2024	Сводная коллекция РГБ	
[12]	3,21%	0%	ЮНиП _ 2 (42)	13 Дек 2019	Сводная коллекция вузов МВД	
[13]	3,21%	0%	ЮНиП _ 2 (42)	29 Дек 2018	Сводная коллекция вузов МВД	
[14]	2,95%	0%	Гатауллин, Зюфяр Шакирович Те... http://dlib.rsl.ru	01 Янв 2022	Сводная коллекция РГБ	
[15]	2,68%	0%	Некоторые проблемы квалифика... http://elibrary.ru	29 Апр 2017	eLIBRARY.RU	
[16]	2,65%	0%	Актуальные проблемы Особенно... http://studentlibrary.ru	20 Янв 2020	Сводная коллекция ЭБС	
[17]	2,58%	0,16%	Хамзяева, Юлия Радиковна Угол... http://dlib.rsl.ru	01 Янв 2017	Сводная коллекция РГБ	
[18]	2,5%	0%	Абисова	04 Июл 2019	Сводная коллекция вузов МВД	
[19]	2,48%	1,55%	Постановление Пленума Верхов... http://ivo.garant.ru	10 Ноя 2016	СПС ГАРАНТ: нормативно-правовая документация	
[20]	2,48%	0%	Постановление Пленума Верхов... http://ivo.garant.ru	10 Ноя 2016	СПС ГАРАНТ: нормативно-правовая документация	
[21]	2,47%	0%	214575 http://biblioclub.ru	18 Апр 2016	Сводная коллекция ЭБС	
[22]	2,46%	0%	Организационно-правовые осно... https://book.ru	01 Янв 2023	Сводная коллекция ЭБС	
[23]	2,46%	0%	Антитеррористическое законода... http://biblioclub.ru	21 Янв 2020	Сводная коллекция ЭБС	
[24]	2,41%	0%	Феоктистов М С	08 Июн 2023	Кольцо вузов	
[25]	2,39%	0%	Террористическая деятельность...	24 Сен 2023	eLIBRARY.RU	
[26]	2,29%	1,53%	не указано	07 Сен 2022	Шаблонные фразы	

[27]	2,19%	0%	ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТ... http://elibrary.ru	01 Янв 2019	eLIBRARY.RU	
[28]	2,15%	0%	Ответственность за финансиров... http://studentlibrary.ru	20 Янв 2020	Сводная коллекция ЭБС	
[29]	2,14%	0%	Petrov A. E. _2020.pdf	26 Мая 2020	Модуль поиска по собственной коллекции	
[30]	2,09%	2,09%	Преступления террористическо... http://elibrary.ru	01 Янв 2023	Публикации eLIBRARY (переводы и перефразирования)	
[31]	2,07%	0%	Зайцев А.В. 2й факультет, группа...	05 Июн 2020	Сводная коллекция вузов МВД	
[32]	1,95%	0%	Основные направления предуп... https://ctarodub.bezformata.com	28 Июн 2023	СМИ России и СНГ	
[33]	1,91%	0%	Игошина А.А. Уголовно-правова...	13 Мая 2019	Кольцо вузов	
[34]	1,86%	0%	Уголовное право России. Части ... http://ivo.garant.ru	27 Фев 2021	СПС ГАРАНТ: аналитика	
[35]	1,8%	0%	Смушкин А.Б. Комментарий к Фе... http://ivo.garant.ru	11 Апр 2015	СПС ГАРАНТ: аналитика	
[36]	1,78%	0,03%	АННОТАЦИЯ К: Использование д... http://ivo.garant.ru	05 Фев 2025	СПС ГАРАНТ: аналитика	
[37]	1,69%	0,49%	Прочитать диссертацию http://test.ssla.ru	30 Янв 2017	Перефразирования по Интернету	
[38]	1,68%	0%	Терроризм: основы уголовной и ... http://ivo.garant.ru	31 Авг 2024	СПС ГАРАНТ: аналитика	
[39]	1,68%	0%	Экологический терроризм как уг... http://elibrary.ru	01 Янв 2015	eLIBRARY.RU	
[40]	1,65%	0%	Правовая основа противодейств... http://klintsy.ru	01 Янв 2019	СМИ России и СНГ	
[41]	1,63%	0,45%	Преступления террористическог...	07 Янв 2025	Кольцо вузов	
[42]	1,56%	0%	ВКР Нефедов	30 Июн 2022	Модуль поиска по собственной коллекции	
[43]	1,56%	0%	Постановление Пленума Верхов... http://kaliningrad.bezformata.ru	03 Янв 2019	СМИ России и СНГ	
[44]	1,56%	0%	Постановление Пленума Верхов... http://sova-center.ru	07 Янв 2019	СМИ России и СНГ	
[45]	1,56%	0%	Постановление Пленума Верхов... http://sova-center.ru	03 Янв 2019	СМИ России и СНГ	
[46]	1,54%	0%	Актуальные проблемы современ... https://book.ru	01 Янв 2024	Сводная коллекция ЭБС	
[47]	1,43%	0%	Туркулец, Валентина Алексеевна... http://dlib.rsl.ru	01 Янв 2023	Сводная коллекция РГБ	
[48]	1,43%	0%	Сборник постановлений Пленум... http://studentlibrary.ru	19 Дек 2016	Медицина	
[49]	1,41%	0%	Сосенков, Федор Сергеевич Пол... http://dlib.rsl.ru	01 Янв 2022	Сводная коллекция РГБ	
[50]	1,33%	0%	Полномочия прокурора в произ... http://studentlibrary.ru	19 Дек 2016	Медицина	
[51]	1,32%	0%	Государство, право, общество в у... http://biblioclub.ru	21 Янв 2020	Сводная коллекция ЭБС	
[52]	1,32%	0%	Учебник Криминалистика Ч.1	23 Ноя 2023	Сводная коллекция вузов МВД	
[53]	1,31%	1,31%	Институциональные основы уго...	19 Окт 2024	Публикации eLIBRARY (переводы и перефразирования)	
[54]	1,23%	0%	МП ЭССЕ Артаг Анужин БМО221....	30 Ноя 2023	Кольцо вузов	
[55]	1,2%	1,2%	Указание Генеральной прокурат... http://ivo.garant.ru	12 Июл 2019	СПС ГАРАНТ: нормативно-правовая документация	
[56]	1,13%	0,66%	ДЕАНОНИМИЗАЦИЯ ПОЛЬЗОВАТ... https://elibrary.ru	19 Апр 2023	eLIBRARY.RU	
[57]	1,13%	0%	Актуальные проблемы расследо... https://book.ru	01 Янв 2023	Сводная коллекция ЭБС	
[58]	1,07%	0%	Актуальные проблемы уголовног... http://studentlibrary.ru	19 Дек 2016	Медицина	
[59]	0,95%	0%	_Юридическая наука и практика...	28 Янв 2025	Сводная коллекция вузов МВД	Источник исключен. Причина: Маленький процент пересечения.
[60]	0,93%	0%	Богданова Д.В._ОНБс-1801б	16 Июн 2023	Кольцо вузов	Источник исключен. Причина: Маленький процент пересечения.
[61]	0,91%	0%	Актуальные проблемы современ... https://book.ru	01 Янв 2023	Сводная коллекция ЭБС	Источник исключен. Причина: Маленький процент пересечения.

[62]	0,87%	0%	Учебник п.34 ПНД ч1	23 Ноя 2023	Сводная коллекция вузов МВД	Источник исключен. Причина: Маленький процент пересечения.
[63]	0,85%	0%	Survey on optical camera commu...	31 Окт 2015	Издательство Wiley	Источник исключен. Причина: Маленький процент пересечения.
[64]	0,81%	0%	Решение Петропавловск-Камчат... http://arbitr.garant.ru	21 Мая 2022	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[65]	0,81%	0%	Уголовное право России. Части ... http://studentlibrary.ru	19 Дек 2016	Медицина	Источник исключен. Причина: Маленький процент пересечения.
[66]	0,81%	0%	ВКР Митрофанова	29 Июн 2020	Модуль поиска по собственной коллекции	Источник исключен. Причина: Маленький процент пересечения.
[67]	0,67%	0%	Citation data as a proxy for qualit...	31 Дек 2016	Издательство Wiley	Источник исключен. Причина: Маленький процент пересечения.
[68]	0,67%	0%	Citation analysis and the develop...	28 Фев 2014	Издательство Wiley	Источник исключен. Причина: Маленький процент пересечения.
[69]	0,67%	0%	Метелев А.В., Образцов В.А., Поз... http://ivo.garant.ru	13 Окт 2018	СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[70]	0,67%	0%	Социальные общности как субъе... http://dep.nlb.by	16 Янв 2020	Диссертации НББ	Источник исключен. Причина: Маленький процент пересечения.
[71]	0,67%	0%	Уголовная ответственность за ф... http://dep.nlb.by	11 Ноя 2016	Диссертации НББ	Источник исключен. Причина: Маленький процент пересечения.
[72]	0,67%	0%	Пятый Пермский конгресс учен... http://studentlibrary.ru	19 Дек 2016	Медицина	Источник исключен. Причина: Маленький процент пересечения.
[73]	0,59%	0%	Финансовая устойчивость перес... http://dep.nlb.by	16 Янв 2020	Диссертации НББ	Источник исключен. Причина: Маленький процент пересечения.
[74]	0,57%	0%	Современные технологии проек... http://habrahabr.ru	25 Дек 2018	СМИ России и СНГ	Источник исключен. Причина: Маленький процент пересечения.
[75]	0,57%	0%	Васильева, Жаргалма Жалсановн... http://dlib.rsl.ru	01 Янв 2013	Сводная коллекция РГБ	Источник исключен. Причина: Маленький процент пересечения.
[76]	0,54%	0%	ushakov_r_m_kvalifikaciya-hishche...	20 Мая 2023	Кольцо вузов	Источник исключен. Причина: Маленький процент пересечения.
[77]	0,54%	0%	Право цифровой среды (монография... http://ivo.garant.ru	20 Авг 2022	СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[78]	0,53%	0%	Антикоррупционное законодате... http://studentlibrary.ru	19 Дек 2016	Медицина	Источник исключен. Причина: Маленький процент пересечения.
[79]	0,53%	0%	Расследование отдельных видов... http://studentlibrary.ru	19 Дек 2016	Медицина	Источник исключен. Причина: Маленький процент пересечения.
[80]	0,53%	0%	ВКР Малющенко (Сай) М.В.	19 Июл 2022	Модуль поиска по собственной коллекции	Источник исключен. Причина: Маленький процент пересечения.
[81]	0,51%	0%	НИР Горбачева	24 Янв 2025	Сводная коллекция вузов МВД	Источник исключен. Причина: Маленький процент пересечения.
[82]	0,49%	0%	Противодействие преступления... http://ivo.garant.ru	18 Мар 2023	СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[83]	0,47%	0%	Приказ МВД России от 25 июня ... http://ivo.garant.ru	30 Янв 2020	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[84]	0,47%	0%	В МВД создано управление по б... https://kommersant.ru	30 Сен 2022	СМИ России и СНГ	Источник исключен. Причина: Маленький процент пересечения.
[85]	0,47%	0%	Петухов, Евгений Николаевич М... http://dlib.rsl.ru	01 Янв 2024	Сводная коллекция РГБ	Источник исключен. Причина: Маленький процент пересечения.
[86]	0,46%	0%	Актуальные вопросы публично-... https://book.ru	01 Янв 2024	Сводная коллекция ЭБС	Источник исключен. Причина: Маленький процент пересечения.
[87]	0,45%	0%	ВКР Травкин С.Л. 12.05.2023	12 Мая 2023	Сводная коллекция вузов МВД	Источник исключен. Причина: Маленький процент пересечения.
[88]	0,4%	0%	Ганбаатар Бигармижид	13 Июл 2021	Модуль поиска по собственной коллекции	Источник исключен. Причина: Маленький процент пересечения.
[89]	0,37%	0%	Афонина, Евгения Григорьевна ... http://dlib.rsl.ru	01 Янв 2024	Сводная коллекция РГБ	Источник исключен. Причина: Маленький процент пересечения.
[90]	0,35%	0%	Верховный суд РФ разъяснил сп... http://ysia.ru	13 Фев 2012	СМИ России и СНГ	Источник исключен. Причина: Маленький процент пересечения.
[91]	0,34%	0%	ИСАЕВ-ВКР	27 Апр 2020	Модуль поиска по собственной коллекции	Источник исключен. Причина: Маленький процент пересечения.
[92]	0,33%	0%	Решение Нижнеингашского райо... http://arbitr.garant.ru	06 Мар 2021	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[93]	0,27%	0%	Проблемы борьбы с организова... http://ivo.garant.ru	17 Сен 2022	СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[94]	0,25%	0%	Теория и практика моделирован... http://dep.nlb.by	20 Дек 2016	Диссертации НББ	Источник исключен. Причина: Маленький процент пересечения.

УДК 343.98

Актуальные проблемы раскрытия и расследования преступлений террористического характера в цифровую эпоху

Мира Николаевна Таршева
Орловский юридический институт МВД России имени В. В. Лукьянова, г. Орел, Российская Федерация, mirra_2023@internet.ru

Аннотация. В статье исследуются отдельные проблемные аспекты, связанные с раскрытием и расследованием террористических преступлений, совершаемых с применением информационных технологий, включая информационно-коммуникационные и информационно-телекоммуникационные средства. Авторы анализируют современные формы и тенденции террористической деятельности. Результаты исследования могут быть полезны для специалистов в области правоохранительной деятельности, информационной безопасности, а также для законодателей, занимающихся вопросами противодействия кибертерроризму.

Ключевые слова: цифровой терроризм, информационные технологии, проблемы раскрытия и расследования ИТ-преступности, кибертерроризм, криптовалюта.

Current problems of disclosure and investigation of terrorist crimes in the digital age

Mira N. Tarsheva Oryol Law Institute of the Ministry of Internal Affairs of Russia named after V. V. Lukyanov, Orel, Russian Federation, mirra_2023@internet.ru

Annotation. The article examines certain problematic aspects related to the disclosure and investigation of terrorist crimes committed using information technology, including information and communication technology and information and telecommunication facilities. The authors analyze modern forms and trends of terrorist activity. The results of the study can be useful for specialists in the field of law enforcement, information security, as well as for legislators dealing with issues of countering cyberterrorism.

Keywords: digital terrorism, information technology, problems of disclosure and investigation of IT crime, cyberterrorism, cryptocurrency.

В современном мире, где цифровые технологии пронизывают все сферы жизни, преступность, в том числе террористическая, приобретает новые формы и масштабы. Цифровая эпоха открыла перед злоумышленниками широкие возможности для организации, координации и сокрытия своей

деятельности, что создает серьезные вызовы для правоохранительных органов. Актуальные проблемы раскрытия и расследования преступлений террористического характера в условиях цифровизации связаны не только с техническими аспектами такой деятельности, но и с необходимостью адаптации правовых, организационных и методологических подходов к новым реалиям. Киберпространство становится ареной для вербовки, финансирования, планирования и осуществления террористических актов, что требует от общества и государства комплексного противодействия, основанного на инновационных технологиях, оптимальном законодательном регулировании, международном сотрудничестве и глубоком понимании трансформирующейся природы угроз. В данной работе рассматриваются ключевые аспекты этой многогранной проблемы, а также возможные пути их решения в условиях стремительного развития информационных технологий.

«За 2024 количество преступлений террористической направленности выросло, причём больше половины из них спланированы и организованы украинскими специальными службами и их кураторами», - озвучил в своем выступлении Президент Российской Федерации В. В. Путин на расширенном заседании коллегии ФСБ России в 2025 году[1].

Что касается цифр, то в 2023 году зарегистрирован[26]382 преступления террористического харак[26]ра (что на [8]7% больше по сравнению с аналогичным показателем прошлог[26]года)[2], в 2024 году - 3714 преступления (что на 55,9% больше по сравнению с АППГ)[3].

Президент отметил, что в сохраняющихся условиях агрессивного настроя части западных элит в отношении нашего государства, направленных на подрыв суверенитета, на откровенный шантаж и запугивание граждан, дестабилизацию, раскол и разобщение нашего общества и пр., необходимо усилить антитеррористическую работу по всем направлениям.

В. В. Путин также подчеркнул, что в последние годы отмечается рост кибератак на отечественную информационную инфраструктуру с причинением ущерба гражданам, бизнесу и государству. Поэтому одной из первоочередных задач органов государственной безопасности (при непосредственной координации Национального антитеррористического комитета) является повышение безопасности отечественной информационной

---

[1] Выступление Президента Российской Федерации на расширенном заседании коллегии ФСБ России в 2025 году. URL: http://www.kremlin.ru/events/president/transcripts/comminity_meetings/76338 (дата обращения: 07.03.2025).

[2] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года // Данные с официального сайта Министерства внутренних дел Российской Федерации. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/?ysclid=m7xn0e4x30695182352 (дата обращения: 06.03.2025).

[3] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // Данные с официального сайта Министерства внутренних дел Российской Федерации. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 06.03.2025).

инфраструктуры, в частности поиск новых и эффективных методов нейтрализации киберугроз.

В законодательстве отсутствуют конкретный перечень террористических преступлений. В доктринальных источниках учеными применяется термин «преступления террористической направленности», а также разработаны несколько подходов к их классификации.

Д. А. Ковлагина считает, что к таким преступлениям следует относить «совершение хотя бы одного из преступлений, предусмотренных статьями 205, 205.1 – 205.5, 208, 211 ч. 4, статьями 220, 221, 277, 278, 279, 360, 361, а также статьями 206, 209, 210, 220, 221, 281, 295, 317, 318 УК РФ, если данные преступления способствуют оказанию воздействия на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом» [1, с. 12].

А. А. Гогин, к примеру, преступления террористической направленности делит на две группы:

– непосредственно террористические (ст. 205, 206, 211, 277, 278, 279, 360, 361 УК РФ);

– вспомогательные, обеспечивающие террористическую деятельность (ст. 205.1, 205.2, 205.3, 205.4, 205.5, 206, 208, 220, 221 УК РФ) [2].

В статистической отчетности Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации используется термин «преступления террористического характера», к которым относятся противоправные общественно-опасные деяния, ответственность за которые предусмотрена:

1) ст. 205, 205.1, 205.2, 205.3, 205.4, 205.5, 205.6, 208, ч. 4 ст. 211, ст. 277, 360, 361 УК РФ;

2) ст. 206, 209, 210, ст. 210.1, ст. 222, 222.1, 223, 223.1, 226, 281, 295, 317, 318, 355 УК РФ – при связи совершенных преступлений с террористической деятельностью;

3) в ряде случаев (в зависимости от даты совершения) – ст. 207, 211, 220, 221, 278, 279, 282.1, 282.2 УК РФ.

Вместе с тем, из текста постановления Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» следует, что к преступлениям террористической направленности суды относят общественно-опасные деяния, запрещенные Уголовным кодексом Российской Федерации под угрозой наказания в соответствии со ст. 205, 205.1, 205.2, 206, 208, 211, 220, 221, 227, 277, 278, 279, 360 УК РФ.

Хотелось бы заметить, что в рамках настоящей работы не ставилась задача представить перечень преступлений террористического характера с обоснованием соответствующих позиций, для целей настоящего исследования этот вопрос не имеет существенного значения.

Научный интерес представляют те преступления террористического характера, совершение которых сопряжено с использованием информационных технологий, на проблемных аспектах раскрытия и расследования которых мы и сосредоточим свое внимание.

Нельзя не заметить, что в юридической литературе, посвященной тематике исследования, употребляются многообразные термины, требующие прояснения: «информационные технологии», «информационно-коммуникационные технологии», «информационно-телекоммуникационные технологии».

Информационные технологии (ИТ) представляют собой широкий спектр методов, процессов и систем, направленных на сбор, обработку, хранение и передачу информации. Этот термин, введенный в научный оборот еще в середине XX века, стал основой для развития современных цифровых систем. Одним из ключевых исследователей в этой области был Клод Шеннон, чья работа «Математическая теория связи» [3] заложила основы теории информации и определила принципы кодирования и передачи данных. Шеннон доказал, что информация может быть количественно измерена, что стало фундаментом для дальнейшего развития ИТ.

С развитием технологий возникло понятие информационно-коммуникационных технологий (ИКТ), которое расширяет рамки ИТ, включая в себя аспекты коммуникации и взаимодействия между пользователями. ИКТ объединяют технологии передачи данных, такие как интернет, мобильная связь и спутниковые системы с традиционными информационными технологиями. Исследования в этой области активно развивались благодаря работам таких ученых, как Винтон Серф и Роберт Кан, создателями протокола TCP/IP, который стал основой современного интернета. Их работа «A Protocol for Packet Network Intercommunication» [4] заложила технические стандарты для глобальной сети.

Информационно-телекоммуникационные технологии (ИТТ) — это более узкое понятие, которое акцентирует внимание на телекоммуникационных аспектах, таких как передача данных на большие расстояния через сети связи. Этот термин часто используется в контексте инфраструктуры связи, включая волоконно-оптические линии, спутниковую связь и беспроводные технологии. Исследования в области ИТТ активно развивались благодаря работам Чарльза Као, получившего Нобелевскую премию за открытие возможности передачи света через оптические волокна. Его работа «Dielectric-fibre surface waveguides for optical frequencies» [5] стала основой для создания современных телекоммуникационных сетей.

Таким образом, хотя ИТ, ИКТ и ИТТ имеют общие корни и взаимосвязаны, они различаются по акцентам: ИТ фокусируются на обработке информации, ИКТ − на взаимодействии и коммуникации, а ИТТ − на технических аспектах передачи данных. Эти различия подчеркивают эволюцию технологий и их специализацию в различных областях применения.

Что касается преступлений террористической направленности, совершаемых с использованием информационных технологий, то нельзя не

заметить, что в научных изданиях для их обозначения применяется разная терминология: «кибертерроризм» [6], «информационный терроризм» [1].

Антонова Е. Ю. выделяет следующие «формы преступной деятельности террористических формирований, совершаемые в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий:

1) распространение идеологии насилия, пропаганда террористической деятельности через цифровое (кибер-) пространство;

2) вербовка новых членов террористических формирований и их обучение;

3) применение цифровых технологий в процессе приготовительной и непосредственной террористической деятельности;

4) цифровые каналы финансирования терроризма» [7].

Интернет-пространство (веб-сайты, чат-форумы, социальные сети) позволяет мгновенно отправлять, обмениваться информацией с неопределенной (достаточно широкой) аудиторией, включая молодежь, которая наиболее уязвима к подобному влиянию. Например, в прямом эфире можно наблюдать за террористическими актами со взрывами или стрельбой, «поглощая» тем самым этот контент; так террористические организации используют Интернет-пространство в пропагандистских целях.

Кроме того, Интернет стал ключевой платформой для вербовки новых членов. Террористические группы используют социальные сети, мессенджеры и специализированные форумы для привлечения сторонников, манипулируя их сознанием и распространяя идеи радикального характера.

ИКТ предоставляют террористам возможности для онлайн-обучения и обмена опытом; террористические организации используют закрытые каналы связи и специализированные ресурсы для обучения своих членов методам изготовления взрывчатых веществ, кибератак и другим преступным действиям. Это делает процесс подготовки террористов более доступным и менее зависимым от географических ограничений.

Для реализации своих целей и обеспечения эффективной деятельности террористические организации активно привлекают значительные материальные, в том числе финансовые ресурсы. Цифровое пространство и современные информационные технологии упрощают процесс финансирования террористической деятельности, делают его более скрытым, что создает дополнительные сложности для правоохранительных органов в борьбе с этим явлением (интернет-банкинг, мобильные переводы, онлайн-торговля, а также использование криптовалют).

Учеными-юристами [8, 9, 10, 11] подробно анализируются методы, способы совершения террористических преступлений с использованием ИТ/ИКТ/ИТТ технологий, которые используют преступники: разработка компьютерных вирусов, «кибербомб» и т.п., использование 3-D принтеров и технологии Deepfake (с помощью которой стало возможным создавать фото-видео снимки, аудиофайлы, которые имеют неотличимое сходство с оригиналом), создание зашифрованных каналов связи, использование сети Интернет и Darknet и пр.

Особую озабоченность (с точки зрения предотвращения террористической деятельности) вызывают современные автономные устройства мирного или военного назначения, управление которыми осуществляется с помощью алгоритмов искусственного интеллекта (далее – ИИ). Существуют опасения, что террористы смогут получить доступ к автономному оружию (дронам, танкам, автомобилям и др. устройствам) и использовать в своих целях. В итоге авторы сходятся на том, что традиционные методы расследования зачастую оказываются недостаточно эффективными в условиях цифровой среды, требуется разработка новых подходов.

Не менее серьезной проблемой следует признать «государственный кибертерроризм» - совершение специальными службами (в том числе кибервойсками, киберполицией и т.д.) развитых в кибернетическом плане стран деяний, выходящих за пределы общеуголовной практики (осуществление хакерских атак на информационные ресурсы, в том числе объекты критически важной информационной инфраструктуры, осуществление киберразведовательных действий, неправомерный сбор информации с различных информационных устройств пользователей (осуществляемый при непосредственном сотрудничестве с владельцами ИТ-продуктов, к примеру «Майкрософт») [12, с. 60-63].

Раскрытие и расследование террористических преступлений, совершенных с использованием ИТ/ИКТ/ИТТ, представляет собой одну из наиболее сложных задач для правоохранительных органов. «… Активное развитие информационной сферы приводит к постоянной адаптации противоправной деятельности к достижениям научно-технического прогресса в информационной сфере» [10].

Одной из ключевых проблем, с которыми сталкиваются правоохранители при раскрытии и расследовании рассматриваемых преступлений, является анонимность, которую предоставляют современные ИКТ. Террористические группы активно используют криптографические технологии и анонимные сети, такие, например, как Tor, для координации своих действий. Это значительно затрудняет идентификацию преступников и сбор доказательств. В этой связи предлагается усилить международное сотрудничество в области противодействия ИТ-преступности, в том числе террористического характера, а также разработать специализированные программные средства для мониторинга и анализа интернет-трафика, в том числе включающие элементы искусственного интеллекта.

Еще одной важной проблемой является недостаточная подготовка сотрудников правоохранительных органов. Многие оперуполномоченные, дознаватели, следователи не обладают необходимыми знаниями в области компьютерных и информационных технологий, что приводит к ошибкам тактического и технического характера (несвоевременность или не проведение следственных и иных процессуальных действий, направленных на получение доказательственной базы; совершение ошибок при изъятии и анализе цифровых следов и электронных данных и т. д).

Для решения этой проблемы предлагалось внедрить в образовательные программы для сотрудников правоохранительных органов курсы по цифровой криминалистике, создать специализированные подразделения, специализирующихся на расследовании ИТ-преступлений, осуществить разработку «рекомендаций и приемов, направленных на повышение эффективности их действий при раскрытии и расследовании данных деяний» для сотрудников органов предварительного расследования [14]. Подобного рода предложения в настоящий момент реализованы на практике. В частности, в 2019 году в структуре МВД России были созданы подразделения, специализирующиеся на расследовании преступлений, совершённых с использованием информационных технологий; в сентябре 2022 года – Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК). УБК стало ведущим подразделением МВД в борьбе с киберпреступностью, задачами которого являются предотвращение, выявление и пресечение преступлений в сфере IT-технологий; анализ данных в информационно-телекоммуникационных сетях в целях выявления запрещённого контента, а также координация действий в рамках ведомства; осуществление взаимодействия с ФСБ, государственными органами, финансовыми учреждениями, организациями, занимающимися информационными технологиями, а также другими участниками информационного обмена, включая агрегаторов данных» .

В 2024 году ФГКУ «Экспертно-криминалистический центр МВД России» и Сбербанк подписали соглашение о сотрудничестве в целях «реализация совместных мероприятий в области научно-исследовательской и научно-технической деятельности, ориентированных на противодействие использованию информационно-телекоммуникационных технологий для совершения противоправных деяний, совершенствование теории и практики цифровой криминалистики, исследование признаков применения технологий подмены личности путем модификации и синтеза аудио- и видеоинформации, а также разработка аппаратно-программных средств, ориентированных на поиск признаков генерации цифрового контента»[4].

Кроме того, российские ученые обращают внимание на необходимость совершенствования законодательной базы. Юристы-правоведы анализируют пробелы в российском законодательстве, которые затрудняют привлечение к ответственности лиц, использующих ИКТ для террористической деятельности, высказываются предложения о внесении изменения в Уголовный кодекс РФ, которые будут предусматривать более строгие санкции за совершение террористических преступлением с использованием ИТ, а также разработать международные соглашения, регулирующие вопросы экстрадиции и обмена информацией между странами. Вместе с тем,

---

[4] ЭКЦ МВД России и Сбербанк подписали соглашение о сотрудничестве // Информация размещена на официальном сайте МВД России. URL: https://xn--b1aew.xn--p1ai/news/item/58905814 (дата обращения: 11.03.2025).

В. А. Мазуров и М. А. Стародубцева, на основе проведенного анализа нормативно-правовых источников, регламентирующих деятельность правоохранительных органов по противодействию кибертерроризму, совершенно справедливо замечают, что в Российской Федерации «… имеет место определенный терминологический вакуум» [6, с. 59], без устранения которого невозможно обеспечение должного международного сотрудничества.

Нельзя не согласиться с позицией ученых, которые считают, что важно учитывать, что борьба с преступлениями террористической направленности, совершаемыми в цифровом (кибер) пространстве или с использованием информационных технологий, не может ограничиваться лишь криминализацией новых общественно опасных деяний или ужесточением наказаний. Ключевым аспектом является глубокое понимание механизмов совершения таких преступлений. Это ставит перед правоохранительными органами новые задачи, требующие умения оперативно выявлять источники террористических угроз и принимать меры для их блокировки или устранения [6, 7, 8, 9].

Таким образом, проблемные вопросы раскрытия и расследования террористических преступлений, совершенных с использованием ИТ, требуют комплексного подхода, включающего совершенствование законодательства, разработку программно-аппаратных комплексов и технологических продуктов по противодействию ИТ-преступности, повышение квалификации сотрудников правоохранительных органов, а также развитие международного сотрудничества в данной сфере (в том числе в области обмена опытом и лучшими практиками, поскольку киберпреступность не знает границ, и борьба с ней требует координации усилий на глобальном уровне). Работы российских ученых в этой области подчеркивают необходимость адаптации традиционных методов расследования к условиям цифровой эпохи.

СПИСОК ИСТОЧНИКОВ:

1. Ковлагина Д. А. Информационный терроризм: понятие, уголовно-правовые и иные меры противодействия: дисс. … канд. юрид. наук. Саратов, 2016. 270 с.

2. Гогин А. А. Понятие, признаки и виды террористических преступлений // Символ науки. 2016 № 12–3 (24). URL: https://cyberleninka.ru/article/n/ponyatie-priznaki-i-vidy-terroristicheskih-prestupleniy (дата обращения: 06.03.2025).

3. Shannon C. E. A Mathematical Theory of Communication (англ.) // Bell System Technical Journal[англ.]: журнал. 1948. Vol. 27. P. 379–423; Шеннон К. Е. Теория связи в секретных системах // Работы по теории информации и кибернетике / Пер. С. Карпова. М.: ИЛ, 1963. 830 с.

4. Cerf, Vinton G. and Robert E. Khan. A Protocol for Packet Network Intercommunication // IEEE Trans on Comms, Vol Com-22, No 5 May 1974. URL: https://networkreviews.wordpress.com/2010/06/30/review-a-protocol-for-packet-network-intercommunication/ (дата обращения: 09.03.2025).

5. Kao K. C., Hockham G. A. Dielectric-fibre surface waveguides for optical frequencies. Proceedings of the Institution of Electrical Engineers, 113(7), 1151–1158. URL: https://www.sci-hub.ru/10.1049/piee.1966.0189 (дата обращения: 10.03.2025).

6. Мазуров В. А. Проблемы противодействия идеологии терроризма и кибертерроризма в современной России: монография / В. А. Мазуров, М. А. Стародубцева; Министерство науки и высшего образования РФ, Алтайский государственный университет. Барнаул: Изд-во Алт. ун-та, 2021. 95 с.

7. Антонова Е. Ю. Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию // Journal of Digital Technologies and Law. 2023. №1. URL: https://cyberleninka.ru/article/n/prestupleniya-terroristicheskoy-napravlennosti-v-epohu-tsifrovizatsii-formy-deyatelnosti-i-mery-po-protivodeystviyu (дата обращения: 11.03.2025).

8. Клебанов Л. Р., Полубинская С. В. Компьютерные технологии в совершении преступлений диверсионной и террористической направленности // Вестник РУДН. Серия: Юридические науки. 2020. №3. URL: https://cyberleninka.ru/article/n/kompyuternye-tehnologii-v-sovershenii-prestupleniy-diversionnoy-i-terroristicheskoy-napravlennosti (дата обращения: 11.03.2025).

9. Колиев В. В., Шахкелдов Ф. Г. Методика раскрытия преступлений, совершаемых с использованием информационно-коммуникационных технологий // Право и практика. 2021. №1. URL: https://cyberleninka.ru/article/n/metodika-raskrytiya-prestupleniy-sovershaemyh-s-ispolzovaniem-informatsionno-kommunikatsionnyh-tehnologiy (дата обращения: 11.03.2025).

10. Информационные технологии в уголовно-правовой сфере: монография / под ред. А.И. Бастрыкина, А.Н. Савенкова. М.: ЮНИТИ-ДАНА, 2023. 279 с.

11. Таршева М. Н. Проблемные вопросы раскрытия и расследования преступлений в сфере информационных технологий / М. Н. Таршева, Л. Д. Матросова // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2024. № 4(101). С. 242-249. EDN VOMATU.

12. Оперативно-розыскная деятельность в цифровом мире: сборник научных трудов /под ред. В. С. Овчинского. Москва, 2024. 630 с.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Таршева Мира Николаевна, кандидат юридических наук, преподаватель кафедры информационных технологий в деятельности ОВД,
Орловский юридический институт МВД России имени В. В. Лукьянова, Российская Федерация, 302027, г. Орел, ул. Игнатова, д. 2.
ORCID 0000-0002-3860-2299
E-mail: mirra_2023@internet.ru

INFORMATION ABOUT THE AUTHOR

Tarsheva Mira Nikolaevna, Candidate of Law, Lecturer at the Department of Information Technology in the Department of Internal Affairs, Oryol Law Institute of the Ministry of Internal Affairs Russia named after V. V. Lukyanov, 2 Ignatova St., Orel, 302027, Russian Federation
ORCID 0000-0002-3860-2299
E-mail: mirra_2023@internet.ru