

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовская государственная юридическая академия»

На правах рукописи

Ковлагина Дарья Александровна

**ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ:
ПОНЯТИЕ, УГОЛОВНО-ПРАВОВЫЕ И ИНЫЕ МЕРЫ
ПРОТИВОДЕЙСТВИЯ**

12.00.08 – уголовное право и криминология,
уголовно-исполнительное право

ДИССЕРТАЦИЯ

на соискание ученой степени
кандидата юридических наук

Научный руководитель:

доктор юридических наук, профессор
Бытко Юрий Ильич

Саратов – 2016

ОГЛАВЛЕНИЕ

Введение.....	3
Глава 1. Терроризм: понятие, формы и виды.....	21
§1. Понятие терроризма в законодательстве и теории	21
§2. Формы и виды терроризма	52
Глава 2. Понятие, признаки и виды информационного терроризма	62
§1. Понятие информационного терроризма: информационное пространство как платформа террористической деятельности	62
§2. Средства (инструменты) информационного воздействия	78
§3. Виды информационного терроризма	99
Глава 3. Уголовно-правовые и иные меры противодействия информационному терроризму	117
§1. Уголовно-правовые меры противодействия информационному терроризму	117
§2. Иные меры противодействия информационному терроризму.....	168
Заключение	182
Список используемых источников.....	192
Приложения	239
Приложение 1	239
Приложение 2	240
Приложение 3	247
Приложение 4	248
Приложение 5	265
Приложение 6	268

ВВЕДЕНИЕ

Актуальность темы исследования. В последнее десятилетие правовым основам обеспечения безопасности информационного пространства от различных вызовов и угроз, в числе которых информационная война, информационный терроризм и информационные преступления, уделяется особое внимание как на уровне законодательства, так и на уровне доктрины. Причиной тому являются глобальные процессы информатизации, а также прогресс в сфере развития информационных технологий.

Современный терроризм характеризуется масштабностью совершаемых террористических акций, высоким уровнем организации и финансирования, резко возросшей технической и технологической оснащенностью (такие террористические организации, как «Хезболла», Хамас и ИГИЛ, имеют сложную структуру, органы управления, свои теле- и радиостанции), что обуславливает появление его новых форм. Кроме того, с каждым годом увеличиваются количественные показатели террористической преступности. Согласно статистическим данным МВД России и Генеральной прокуратуры РФ, за первое полугодие 2016 г. было зарегистрировано 1313 преступлений террористической направленности, что на 73,4% больше, чем за аналогичный период предыдущего года¹.

Информационный терроризм как одна из форм современного терроризма известен российским ученым еще с начала XXI века, но до сих пор нет определенности в понимании его сущности и основных признаков. Между тем в условиях глобализации общество нуждается в правовом

¹ См.: Краткая характеристика состояния преступности в Российской Федерации за январь – июнь 2016 года [Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации. URL: <https://xn--b1aew.xn--p1ai/folder/101762/item/8127775/> (дата обращения: 01.09.2016); Состояние преступности в России за январь – июнь 2016 года. Ежемесячный сборник за июнь 2016 года [Электронный ресурс] // Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: <http://crimestat.ru/analytics> (дата обращения: 01.09.2016).

осмыслении отношений, складывающихся в новой сфере, а также в защите информационного пространства. На сегодняшний день отечественное законодательство в сфере обеспечения информационной безопасности развито слабо и в значительной мере отстает от уровня развития информационного общества.

Согласно Доктрине информационной безопасности Российской Федерации², основные направления государственной политики в этой сфере должны быть связаны с принятием уголовно-правовых, гражданско-правовых, административно-правовых мер противодействия возможным угрозам. Следует сказать, что в последнее время в Российской Федерации было разработано значительное количество документов, регламентирующих вопросы обеспечения защиты информационного пространства. Между тем большинство из них не имеют определенного юридического статуса, а положения, в них закрепленные, не находят своего отражения в содержании российского законодательства.

Названные обстоятельства затрудняют возможность создания общих профилактических, предупредительных и специальных уголовно-правовых, административно-правовых, организационных, экономических, технических, технологических и иных мер противодействия информационному терроризму.

В современных условиях угрозы информационного терроризма стали реальностью, что обусловлено глобальными процессами информатизации, связанными с повсеместной автоматизацией всех объектов жизнеобеспечения, инфраструктуры государств, возрастанием влияния информации на все сферы жизнедеятельности общественных и государственных структур и интеграцией страны в международный информационный обмен. Эксперты Центра исследований борьбы с компьютерной преступностью не исключают возможности

² Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Рос. газета. 2000. 28 сент.

несанкционированного вторжения злоумышленников в системы управления и контроля, направленного на отключение или разрушение государственной или корпоративной инфраструктуры, которые могут повлечь последствия, сравнимые с последствиями традиционного террористического акта, совершенного посредством взрыва, поджога и т.д.³; а массированное воздействие на психику людей с использованием средств массовой информации, информационно-телекоммуникационных сетей (в том числе сети Интернет) может стать регулятором поведения не только отдельного индивида, но и социальной группы и даже общества в целом. Информационное пространство используется террористическими организациями (сообществами) в целях вмешательства в информационно-технологические системы крупных организаций и предприятий, финансирования террористической деятельности, установления связей между террористами, организации деятельности террористических организаций (сообществ), пропаганды, вербовки и т.п.

Недостаточное нормативное регулирование отношений в сфере обеспечения информационной безопасности, отсутствие необходимой научной разработанности проблем уголовно-правового противодействия информационному терроризму, а равно активное использование информационного пространства террористическими организациями (сообществами) предопределили актуальность и выбор темы настоящего диссертационного исследования.

Степень научной разработанности проблемы. Некоторые вопросы, связанные с противодействием угрозам в информационном пространстве, были рассмотрены в работах В.А. Голубева, Д.А. Журавлева, А.В. Кубышкина, Е.Н. Молодчей, И.Н. Панарина, Л.Г. Панариной,

³ См.: Голубев В.А. Проблемы борьбы с кибертерроризмом в современных условиях [Электронный ресурс] // Центр исследования проблем компьютерной преступности. URL: <http://www.crime-research.org/library/e-terrorism.htm> (дата обращения: 15.08.2016).

И.М. Рассолова, Е.А. Роговского, Д.А. Соломина, Е.В. Старостиной, Т.Л. Тропиной, М.И. Шамова и других авторов.

Однако до настоящего времени попыток всестороннего уголовно-правового и криминологического изучения информационного терроризма не предпринималось. Проведенный анализ диссертационных и иных монографических исследований свидетельствует о смешении явления информационного терроризма с кибернетическим терроризмом или психологическим терроризмом.

Криминологические и уголовно-правовые аспекты проблем сущности и содержания терроризма были рассмотрены в работах Ю.М. Антоняна, Т.С. Бояр-Созонович, В.И. Василенко, В.В. Витюка, С.И. Грачева, Ю.Н. Дерюгиной, С.У. Дикаева, В.П. Емельянова, Е.П. Ильина, В.Н. Кудрявцева, В.В. Лунеева, А.А. Лунёва, Л.А. Моджорян, М.Ф. Мусаеляна, В.Е. Петрищева, Д.В. Сопова, М.П. Требина, В.А. Федорцева, С.А. Эфирова и других авторов. Труды названных ученых носят фундаментальный характер, в том числе важны для настоящего исследования, однако терроризм в них рассматривался в общем, без направленности на специфику информационного терроризма.

Среди специалистов, изучающих вопросы пропагандистского воздействия терроризма на сознательно-волевые компоненты личности, социальных групп и общества в целом с помощью средств массовой информации, сети Интернет и иных средств коммуникации, следует отметить О.Н. Алексеева, М.Ю. Великосельского, Д.А. Журавлева, Е.П. Ильина, Д.В. Ольшанского, М.И. Шамова и др.

Объектом диссертационного исследования является информационный терроризм, а также общественные отношения, складывающиеся в связи с установлением и реализацией уголовно-правовых и иных мер противодействия ему.

Предмет исследования составляют применимые к объекту исследования нормы и положения международно-правовых документов и

зарубежных нормативных актов, Уголовного кодекса РФ, отечественных федеральных законов и иных нормативно-правовых актов, а также материалы судебной практики.

Цель и задачи исследования. *Цель* исследования состоит в формировании концептуального представления о понятии, средствах (инструментах) и видах информационного терроризма, а также в выработке с учетом полученных данных научно обоснованных рекомендаций по повышению эффективности уголовно-правовых и иных мер противодействия ему.

Для достижения данной цели были поставлены следующие *задачи*:

- выявить существенные признаки таких исходных понятий, как «терроризм» и «информация», и сформулировать на их основе дефиниции указанных понятий;
- определить соотношение понятий «терроризм», «террористическая деятельность» и «преступления террористической направленности»;
- установить критерии выделения информационного терроризма как формы терроризма;
- раскрыть содержание отличительных признаков информационного терроризма и основания разделения его на виды;
- обосновать общественную опасность информационного терроризма;
- разработать предложения по совершенствованию уголовного законодательства с целью эффективного противодействия информационному терроризму;
- предложить комплекс иных мер противодействия информационному терроризму, направленных на его профилактику и предупреждение.

Теоретическая база исследования. Рассмотрение особенностей информационного терроризма и формирование научно обоснованного комплекса мер противодействия ему осуществляется в работе с учетом достижений таких отраслей юридической науки, как теория государства и права, международное право, уголовное право, криминология и др.

В ходе исследования учитывались научные разработки ученых, внесших неоценимый вклад в общую теорию права: М.И. Байтина, В.Л. Кулапова, А.В. Малько, Н.И. Матузова и др.

Немаловажным было использование работ ученых, имеющих фундаментальное значение для развития науки уголовного права и криминологии: А.В. Бриллиантова, А.Г. Блинова, Ю.И. Бытко, А.Н. Варыгина, Г.В. Вериной, Л.Д. Гаухмана, Я.И. Гилинского, А.И. Долговой, Н.А. Лопашенко, Б.Т. Разгильдиева и др.

Специфика научной проблематики обусловила обращение к работам исследователей, специализирующихся на проблеме определения сущности терроризма и противодействия ему: Ю.М. Антоняна, В.И. Василенко, С.И. Грачева, С.У. Дикаева, В.П. Емельянова, А.И. Коробеева, В.Н. Кудрявцева, А.А. Курбанмагомедова, С.М. Кочои, В.В. Лунеева, А.А. Лунёва, Л.А. Маджорян, М.Ф. Мусаеляна, В.Е. Петрищева, Д.В. Сопова, Д.И. Тисленко, М.П. Требина, В.А. Федорцева и др.

Помимо названных работ теоретической базой диссертационного исследования послужили труды авторов, научная деятельность которых связана с разработкой мер противодействия различным угрозам в киберпространстве: В.А. Голубева, Р.И. Дремлюги, Д.А. Журавлева, Е.Н. Молодчей, Е.А. Роговского, Е. Старостиной, Т.Л. Тропиной и др.

Диссертант также обращался к исследованиям, раскрывающим вопросы обеспечения международной информационной безопасности и противодействия терроризму в информационной сфере, в частности А.В. Кубышкина, Д.А. Соломина, М.И. Шамова.

В связи с изучением вопросов информационного воздействия закономерным было обращение к исследованиям таких авторов, как М.Ю. Великосельский, Д.А. Журавлев, Е.П. Ильин, Л.А. Колобов, В.Е. Петрищев, А.А. Робинов, А.В. Столяров и др.

При определении сущности информации как одного из инструментов информационного воздействия были проанализированы работы И.Л. Бачило,

Л.А. Букалеровой, А.Н. Григорьева, А.Н. Колмогорова, В.Г. Степанова-Егиянц, А.А. Турышева, А.Д. Урсула, И.А. Яковлевой, С.А. Яшкова и др.

Правовую базу исследования образуют Конституция РФ, Уголовный кодекс РФ, федеральные законы («О противодействии терроризму», «Об информации, информационных технологиях и защите информации» и др.) и иные нормативно-правовые акты России. Особое внимание уделено анализу международно-правовых документов, а также уголовного законодательства зарубежных стран (Республики Казахстан, Республики Узбекистан, Украины, Великобритании, США).

Методология диссертационного исследования. При проведении исследования широко использовались категории и принципы диалектического метода познания явлений и процессов окружающей действительности, а также основанные на нем общенаучные методы (анализ, синтез, индукция, дедукция, абстрагирование, логический, системный и др.), специальные юридические методы (сравнительно-правовой, историко-правовой, формально-юридический, правового моделирования и др.) и методы эмпирического уровня (обобщения судебной практики, уголовно-статистический, интервьюирования, анкетирования).

Эмпирическая основа диссертационного исследования представлена:

- результатами изучения 94 приговоров, вынесенных судами за период с 2012 г. по первое полугодие 2016 г. на территории 9 республик (Башкортостан, Дагестан, Кабардино-Балкарская, Карелия, Саха, Татарстан, Удмуртская, Хакасия, Чувашия), 7 краев (Алтайский, Забайкальский, Краснодарский, Красноярский, Пермский, Ставропольский, Хабаровский), 26 областей (Амурская, Архангельская, Астраханская, Белгородская, Воронежская, Владимирская, Кемеровская, Кировская, Костромская, Курская, Ленинградская, Московская, Новосибирская, Орловская, Самарская, Саратовская, Свердловская, Тамбовская, Тверская, Томская, Тульская, Тюменская, Ульяновская, Челябинская, Ярославская) по уголовным делам о

преступлении, предусмотренном ст. 207 УК РФ;

- результатами изучения 60 приговоров, вынесенных судами за период с 2015 г. по май 2016 г. на территории 5 республик (Калмыкия, Карелия, Марий Эл, Саха, Удмуртская), 2 краев (Забайкальский, Красноярский), 12 областей (Владимирская, Ивановская, Калужская, Кемеровская, Кировская, Курганская, Московская, Ростовская, Самарская, Томская, Тамбовская, Тюменская) и 2 автономных округов (Ханты-Мансийский, Ямало-Немецкий) по уголовным делам о преступлении, предусмотренном ст. 273 УК РФ;

- результатами анкетирования 167 жителей городов Балакова, Нальчика, Саратова, Ставрополя, Черкесска, занятых в различных сферах жизнедеятельности (преподаватели, сотрудники правоохранительных органов, государственные и муниципальные служащие, пенсионеры, студенты), проведенного в 2014-2015 гг. на тему: «Информационный терроризм как современная угроза: общественное мнение»;

- результатами интервьюирования 19 экспертов - специалистов в области уголовного права и криминологии (в их числе 2 доктора юридических наук и 14 кандидатов юридических наук по специальности 12.00.08) в целях подтверждения основных результатов, полученных автором в процессе изучения явления информационного терроризма, разработки уголовно-правовых и иных мер противодействия ему;

- данными официальной статистики о преступлениях террористической направленности за период с 2015 г. по первое полугодие 2016 г.

Научная новизна диссертационной работы состоит в том, что в результате проведенного исследования сформировано концептуальное представление о понятии, средствах (инструментах), видах информационного терроризма и на основе полученных данных разработан комплекс предложений, направленных на оптимизацию уголовно-правовых и иных мер противодействия ему.

Свое выражение научная новизна диссертации получает в следующих **положениях, выносимых на защиту.**

1. Понятие «терроризм» является общеправовым, родовым понятием, которое получает свою конкретизацию в понятии террористической деятельности. Преступления (правонарушения) террористической направленности представляют собой конкретные формы проявления террористической деятельности.

Терроризм характеризуется следующими сущностными признаками:

- он представляет собой практику воздействия;
- воздействие является идеологически обоснованным;
- воздействие сопряжено с устрашением населения;
- воздействие имеет опосредованный характер: имущественный, физический и иной вред причиняется одним лицам (тактические объекты), а воздействие осуществляется на других (стратегические объекты).

Терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом.

Данную дефиницию необходимо закрепить в статье 3 Федерального закона от 06.03.2006 № 35-ФЗ «О противодействии терроризму».

2. Террористическая деятельность обладает следующими сущностными признаками:

- деятельный характер (это всегда поведенческие акты);
- противоправность;
- выраженность в совершении преступлений или правонарушений террористической направленности.

Террористическая деятельность – это запрещенная Уголовным кодексом РФ и (или) Кодексом РФ об административных правонарушениях деятельность, выражающаяся в совершении деяний террористической направленности.

Данное определение следует закрепить в статье 3 Федерального закона от 06.03.2006 № 35-ФЗ «О противодействии терроризму». Между тем оно требует конкретизации в Уголовном кодексе Российской Федерации (далее – УК РФ) для целей его недвусмысленного понимания в контексте некоторых составов преступлений. С этой целью ст. 205¹ УК РФ должна быть дополнена примечанием 1.2 следующего содержания: «Под террористической деятельностью в статьях настоящего Кодекса следует понимать совершение хотя бы одного из преступлений, предусмотренных статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, 211 ч. 4, статьями 220, 221, 277, 278, 279, 360, 361, а также статьями 206, 209, 210, 220, 221, 281, 295, 317, 318 настоящего Кодекса, 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».

3. Преступления (правонарушения) террористической направленности – это общественно опасные, противоправные деяния, запрещенные Уголовным кодексом РФ и (или) Кодексом РФ об административных правонарушениях, которые оказывают или способствуют оказанию воздействия на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом.

Данную дефиницию следует изложить в статье 3 Федерального закона от 06.03.2006 № 35-ФЗ «О противодействии терроризму».

4. Информационный терроризм имеет следующие отличительные признаки:

- платформой информационного терроризма выступает информационное пространство, т.е. характеризующаяся безграничностью сфера существования общественных отношений, связанная с использованием информации, информационных технологий и информационных ресурсов;

- инструментами (средствами) воздействия выступают информация, информационные ресурсы и (или) информационные технологии.

Информационный терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах информационного пространства, связанного с использованием информации, информационных технологий и (или) информационных ресурсов.

5. Сущностные признаки информации:

- информация – это сведения;
- информация – это сведения, обладающие информационной ценностью, то есть имеющие значение для достижения определенного преступного результата;
- информация находится на определенных носителях, которыми могут выступать сам человек, бумажные, аудио-, видеоносители и др.;
- использование информации как предмета или средства («орудия») направлено на достижение преступных целей.

Информация как предмет или средство («орудие») преступления – это сведения, находящиеся на определенном носителе, обладающие информационной ценностью для своего потребителя или пользователя, использование которых необходимо для достижения преступных целей.

6. Детальное исследование проблем противодействия информационному терроризму, а также повышение эффективности такого противодействия возможно лишь путем выделения его видов, которыми следует признать информационно-психологический терроризм и информационно-технологический терроризм.

Информационно-психологический терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом

местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах информационного пространства путем совершения действий, связанных с использованием информации и оказанием влияния на сознательно-волевые компоненты личности (социальной группы либо представителя власти).

Информационно-психологическое воздействие может осуществляться в пределах всего информационного пространства, составляющими компонентами которого являются информация, информационные технологии и информационные ресурсы.

Информационно-технологический терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, юридическим лицом, социальной группой или физическим лицом в пределах киберпространства, связанная с совершением противоправных действий в отношении отдельных компонентов информационной среды и (или) инфраструктуры государств либо организаций с помощью информационных технологий и (или) цифровых информационных ресурсов.

Информационно-технологическое воздействие может осуществляться только в пределах киберпространства, являющегося частью информационного пространства. Киберпространство представляет собой сферу существования общественных отношений, доступ к которой обеспечивается с помощью различных технических устройств, объединенных сетью Интернет или иной локальной или территориальной сетью, связанной с использованием информационных технологий, компьютерной информации и цифровых информационных ресурсов.

7. Диспозицию части 1 статьи 205 УК РФ необходимо изложить в следующей редакции:

«Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения

значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом, либо физическим лицом и дестабилизации деятельности органа власти, органа местного самоуправления или международной организации, а также угроза совершения указанных действий в тех же целях, -

наказываются...»

Дестабилизация деятельности органа власти, органа местного самоуправления или международной организации как цель террористического акта всегда объективно существует наряду с целью воздействия на принятие решения или совершения действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом. Воздействие, в свою очередь, проявляется не только в предъявлении требований, но и во взятии на себя ответственности за совершенные террористические акты, что демонстрирует влияние, силу и власть террористических групп (организаций или сообществ).

В целях повышения эффективности уголовно-правового противодействия информационно-технологическому терроризму в части 2 статьи 205 УК РФ необходимо предусмотреть пункт «г» следующего содержания:

«сопряженные с посягательством на автоматизированные системы критически важных объектов и (или) потенциально опасных объектов государства, создающие опасность гибели человека, причинения значительного имущественного ущерба, аварийной ситуации, техногенной аварии либо иных тяжких последствий, с помощью информационных технологий, -

наказываются...».

8. В связи с активным использованием информации для целей совершения террористических преступлений необходимо внести изменения в содержание статей 272 и 273 УК РФ:

- часть 2 статьи 272 УК РФ изложить в следующей редакции:

«То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, а равно с целью скрыть другое преступление или облегчить его совершение, -

наказывается ...».

- преступление, предусмотренное статьей 273 УК РФ, следует признать равным по характеру и степени общественной опасности с преступлением, предусмотренным ст. 272 УК РФ, в связи с чем:

1) расположить квалифицированные составы преступлений в статье 273 УК РФ в той же последовательности, что и в статье 272 УК РФ, установив максимальное наказание по части 2 – до четырех лет лишения свободы, по части 3 – до пяти лет лишения свободы, по части 4 – до семи лет лишения свободы;

2) изложить часть 2 статьи 273 УК РФ в следующей редакции:

«Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, а равно с целью скрыть другое преступление или облегчить его совершение, -

наказываются...».

9. В целях оптимизации уголовно-правового противодействия информационно-психологическому терроризму следует внести некоторые изменения в УК РФ, а именно: часть 1 статьи 205² УК РФ изложить в следующей редакции:

«Публичное оправдание террористической деятельности либо публичные призывы к осуществлению террористической деятельности, а равно распространение, изготовление, хранение, перевозка, ввоз на территорию Российской Федерации или вывоз с территории Российской Федерации в целях распространения материалов с такими призывами либо

материалов, оправдывающих осуществление террористической деятельности, -

наказываются...».

Следует признать неудачным содержание диспозиции части 2 статьи 205² УК РФ в части указания в ней на использование электронных сетей наравне с информационно-телекоммуникационной сетью, поскольку понятие «электронные сети» входит в содержание понятия «информационно-телекоммуникационные сети». В связи с этим предлагаем изложить часть 2 статьи 205² УК РФ в следующей редакции:

«Те же деяния, совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети "Интернет"», -

наказываются...»

Примечание 1 к статье 205² УК РФ изложить в следующей редакции (изменения выделены курсивом):

«В настоящей статье под публичным оправданием *террористической деятельности* понимается *публичное признание террористической деятельности* правильной, нуждающейся в поддержке и подражании.»

Примечание 2 к статье 205² УК РФ изложить следующим образом: «В настоящей статье под террористической деятельностью понимается совершение хотя бы одного из преступлений, предусмотренных статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, 211 ч.4, 220, 221, 277, 278, 279, 360, 361 настоящего Кодекса».

10. К комплексу иных мер противодействия информационному терроризму следует относить:

- разработку и совершенствование специализированного понятийного аппарата в сфере обеспечения информационной безопасности путем принятия и внесения изменений в правовые акты, регламентирующие вопросы защиты информации и правомерного использования информационных технологий;

- повышение эффективности сотрудничества органов и структур, направление деятельности которых связано с противодействием терроризму, с Управлением «К» МВД России, иными специализированными подразделениями, связанными с обеспечением безопасности информационно-телекоммуникационных сетей, а также с негосударственными учреждениями и организациями, деятельность которых связана с обеспечением внутренней информационной безопасности;

- разработку условий сотрудничества специализированных структур с негосударственными организациями саморегулирования средств массовой информации по вопросу выявления публикаций, возбуждающих ненависть или вражду в отношении каких-либо социальных групп, а также публикаций, оказывающих поддержку или оправдывающих террористическую деятельность, и т.п.;

- развитие и совершенствование кадрового обеспечения информационной безопасности;

- совершенствование системы внутренней информационной защиты учреждений и организаций от возможных посягательств с помощью сети Интернет (иной локальной или территориальной сети), а также иных информационных технологий;

- установление и укрепление международного сотрудничества государств в сфере обеспечения информационной безопасности от возможных угроз террористического характера;

- иные меры превентивного характера, связанные с формированием у населения негативного отношения ко всем возможным проявлениям терроризма, к использованию насилия для достижения целей терроризма и экстремизма.

Теоретическая значимость исследования заключается в том, что разработанные в результате его проведения положения и выводы формируют новое научное знание об информационном терроризме и мерах уголовно-правового и иного противодействия ему, способствуя тем самым развитию

российской уголовно-правовой и криминологической науки, а также могут служить основой для дальнейших исследований указанных проблем.

Практическая значимость исследования определяется тем, что содержащиеся в нем положения, выводы и рекомендации могут оказаться полезными в деятельности по оптимизации уголовного и иного законодательства в сфере противодействия терроризму, в работе правоохранительных органов по обеспечению защиты информационного пространства от террористических и иных возможных угроз, а равно в учебном процессе юридических вузов (факультетов, институтов) в рамках преподавания курсов Особенной части уголовного права и криминологии.

Апробация результатов исследования. Диссертация прошла обсуждение и получила одобрение на кафедре уголовного и уголовно-исполнительного права ФГБОУ ВО «Саратовская государственная юридическая академия».

Основные научные результаты диссертации отражены в 9 научных статьях общим объемом 2,4 а.л., три из которых размещены в изданиях, рекомендованных ВАК при Минобрнауки России.

Основные положения, содержащиеся в диссертации, озвучены в докладах на научно-практических мероприятиях, в частности: Международной научно-практической конференции, посвященной 20-летию Конституции Российской Федерации (в рамках VI Саратовских правовых чтений, Саратов, 2013), Международной научно-практической конференции «Уголовная политика и проблемы правоприменения» (Санкт-Петербург, 2013), XI Международной научно-практической конференции «Татищевские чтения: актуальные проблемы науки и практики» (Тольятти, 2014), VI Всероссийской научно-практической конференции молодых ученых, аспирантов, магистрантов и студентов, посвященной 85-летию ФГБОУ ВО «Саратовская государственная юридическая академия» «Актуальные вопросы современной юридической науки» (Балаково, 2015), Саратовских правовых чтениях: «Уголовно-правовое воздействие и его роль в

предупреждении преступности» (Саратов, 2016), IX Международной научно-практической конференции, посвященной 80-летию Саратовской области: «Политико-правовые проблемы взаимодействия власти, общества и бизнеса в условиях экономического кризиса» (Саратов, 2016).

Структура диссертации. Диссертация состоит из введения, трех глав, содержащих семь параграфов, заключения, библиографического списка и приложений.

ГЛАВА 1. ТЕРРОРИЗМ: ПОНЯТИЕ, ФОРМЫ И ВИДЫ

§1. Понятие терроризма в законодательстве и теории.

Понятие «терроризм» появилось более 200 лет назад, и уже тогда оно имело неоднозначный смысл. Непродолжительное время слово «террорист» использовалось в положительном значении. Однако уже в годы третьего этапа Великой французской революции (1793 – 1794 гг.) терроризм означал «правление ужаса»⁴.

Изначально зародившееся как национальное явление, на сегодняшний день терроризм представляет опасность для всего мирового сообщества⁵, о чем свидетельствует многообразие международных документов, так или иначе содержащих в себе вопросы, связанные с определением его сущности, мер противодействия и с привлечением к ответственности лиц, совершивших террористические преступления.

На протяжении многих лет на международном уровне предпринимались попытки объяснить, что представляет собой терроризм, которые чаще сводились к перечислению конкретных общественно опасных деяний, угрожающих жизни, телесной неприкосновенности, здоровью человека и т.п.⁶ Адекватная невозможность формулирования единого понятия терроризма на международном уровне обусловлена различными внутригосударственными подходами к пониманию сущности данного явления, а также его изменчивым и многоаспектным характером⁷.

⁴ См.: История появления терроризма [Электронный ресурс]. URL: <http://www.privacyandterrorism.org/history.php> (дата обращения: 11.04.2016).

⁵ См.: Коробеев А.И., Лобач Д.В. Терроризм, экстремизм в современной Мексике // Азиатско-Тихоокеанский регион: экономика, политика, право. 2014. № 1 (30). С. 132.

⁶ III Международная конференция по унификации уголовного законодательства. Брюссель. 1930 г. См.: Трайнин А.Н. Избранные произведения. Защита мира и уголовный закон / под ред. Р.А. Руденко. М.: Наука. 1969. С. 40-41.

⁷ Несмотря на это, некоторые исследователи настаивают на необходимости выработки единого, общепринятого понятия терроризма. См.: Карпец И.И. Международная преступность. М.: Наука. 1988. С. 12; Бояр-Созонович Т.С. Международный терроризм: политико-правовые аспекты. Киев-Одесса: «Лыбидь». 1991. С. 119-120; Григорьев А.А. Уголовно-правовая ответственность за терроризм в современном праве Российской Федерации: дис. ... канд. юрид. наук. Челябинск, 2012. С. 40-41.

За 200 лет характер террористических актов изменялся в связи с усовершенствованиями в сфере вооружений. С появлением и испытанием первой атомной бомбы возникла угроза ядерного терроризма. С возникновением химического и бактериологического оружия, соответственно, возникла угроза использования их террористами.

В настоящее время супертерроризм стал реальностью. Но не только появление и совершенствование заведомо опасных физических, химических, биологических и других объектов приводит к угрозе использования их негосударственными субъектами в террористических целях. Развитие информационных технологий, позволяющих быстро производить различного рода операции с информацией (такие как, передача, модификация, уничтожение, блокирование и др.), компьютеризация всех государственных и негосударственных структур, дешевизна и относительная простота доступа к информационно-телекоммуникационным системам, в том числе к сети «Интернет», способствовали возникновению новой сферы преступной деятельности.

Однако, прежде чем говорить о сущности и общественной опасности информационного терроризма и о способах использования информации террористическими группами (организациями или сообществами), необходимо проанализировать уже существующее в зарубежном и, в особенности, отечественном законодательстве понятие «терроризм», а также определить его место среди таких понятий, как «террористическая деятельность» и «преступления террористической направленности».

Терроризм происходит от слова «террор», что означает «страх, ужас». Толковый словарь русского языка определяет «террор» как «политику устрашения, подавления политических противников насильственными мерами»⁸. Однако О.В. Будницкий считает, что использование понятий «терроризм» и «террор» как синонимов, ссылаясь на этимологию, ошибочно. Террор – способ действия любого субъекта (государства, организации,

⁸ См.: Ожегов С.И. Словарь русского языка. 17-е изд., стереотип. М.: Русский язык, 1985. С. 691.

физического лица) с использованием силы, угрозы, возбуждения страха⁹. Подразумевается, что террор в большей степени характерен для субъектов власти¹⁰.

На сегодняшний день дискуссионным является вопрос о необходимости формулирования понятия терроризма. Ряд исследователей полагают, что терроризм – слишком сложное социальное явление, дать определение которого затруднительно¹¹.

В некоторых зарубежных странах нет законодательно закрепленного понятия терроризма, как, впрочем, и нет понятия информационного терроризма, являющегося предметом изучения данного диссертационного исследования, хотя их уголовное законодательство предусматривает ответственность за преступления террористического характера. Однако нет сомнений в том, что разработка такого понятия, в первую очередь – на национальном уровне, конкретизировала бы, какие преступные деяния относятся к терроризму.

Терроризм является сложным, многоаспектным и изменчивым явлением. Изучением феномена терроризма занимаются ученые различных областей знаний (социологи, политологи, криминологи, психологи и др.). Представляется, что всестороннее исследование данного негативного явления, его последствий, а также предупреждение возможно лишь после разработки отвечающего требованиям общественного развития понятийного аппарата.

В настоящее время помимо стран, которые не разработали на национальном уровне закон о борьбе с терроризмом (такие как Словакия, Швейцария, Швеция, ФРГ), существуют и такие страны, как Алжир, где

⁹ См.: Будницкий О.В. История терроризма в России в документах, библиографиях, исследованиях: учебное пособие. Ростов-на-Дону: Феникс, 1996. С. 128.

¹⁰ См.: Гилинский Я.И. Криминология: теория, история, эмпирическая база, социальный контроль. СПб.: Алеф-Пресс. 2014. С. 282.

¹¹ См.: National Advisory Committee on Criminal Justice Standards and Goals, Disorders and Terrorism. Report of the Task Force on Disorders and Terrorism. Washington, DC: U.S. Government Printing Office, 1976. XXIV. P. 10; Тимофеева Н.Ю. К вопросу об определении терроризма в работах зарубежных правоведов // Государство и право России: история и современность. 2008. № 3. С. 88.

меры противодействия терроризму и сам терроризм включены в документы с грифом «секретно», и Япония, в законодательстве которой продолжительное время отсутствовало как понятие терроризма, так и сама ответственность за террористическую деятельность. Показательным в этом отношении является уголовное дело по факту акции экологического терроризма в марте 1995 года в токийском метро, когда виновному вменялись такие преступления, как убийство и покушение на убийство (погибли 12 человек, пострадали свыше 5 тысяч)¹².

Несмотря на действительно существующую трудность в формулировании понятия терроризма, обусловленную различными факторами, мы согласимся с такими российскими исследователями как В.В. Витюк и С.А. Эфиров, подтверждающих возможность и необходимость его определения¹³.

В законодательстве некоторых зарубежных стран, в том числе бывших республик СССР, понятие терроризма характеризуется как активное проявление поведения виновного (-ых) лица (лиц) во внешнем мире.

Так, Уголовный кодекс Республики Узбекистан в ст. 155 устанавливает, что терроризм – это «насилие, использование силы, иные деяния, создающие опасность для личности или собственности, либо угроза их осуществления...»¹⁴.

Закон Украины «О борьбе с терроризмом» раскрывает понятие терроризма через понятие общественно опасной *деятельности*¹⁵.

В законодательстве Великобритании под терроризмом понимается *совершение или угроза совершения действий*, связанных с применением

¹² См.: Уголовное право зарубежных стран. Общая и Особенная части: учебник для магистров / Н.А. Голованова, Е.В. Еремин, М.А. Игнатова [и др.]; под ред. Н.Е. Крыловой. 4-е изд., перераб. и доп. М.: Изд-во Юрайт, 2013. С. 1020.

¹³ См.: Витюк В.В., Эфиров С.А. «Левый» терроризм на Западе: история и современность. М.: Наука, 1987. С. 222-223; Катрич Л.В. Проблема определения терроризма: социолингвистический анализ // Вестник Нижегородского университета им. Н.И. Лобачевского. 2009. № 1. С. 19.

¹⁴ См.: Уголовный Кодекс Республики Узбекистан [Электронный ресурс]. URL: http://www.lex.uz/pages/getact.aspx?lact_id=111457 (дата обращения 15.03.2016).

¹⁵ См.: Закон Украины «О борьбе с терроризмом» [Электронный ресурс]. URL: <http://zakon1.rada.gov.ua/laws/show/638-15> (дата обращения: 15.03.2016).

существенного насилия в отношении лица; с причинением значительного ущерба имуществу и т.д.¹⁶ Федеральное уголовное законодательство США определяет терроризм как деятельность¹⁷.

В российской доктрине на сегодняшний день сложились различные точки зрения на понимание сущности терроризма. Такие исследователи, как В.А. Федорцев¹⁸, М. Вершинин¹⁹, говоря о терроризме, характеризуют его как *метод* достижения террористических целей. Примерно также – как метод воздействия на органы государственной власти – объясняет понятие терроризма в своих научных трудах Н.Н. Гриб²⁰. Но подобная трактовка понимания терроризма довольно-таки спорна. Скорее следует расценивать насилие и иные формы противоправного воздействия, выступающие как существенный признак терроризма, в качестве методов (способов, средств) достижения террористических целей. Кроме того, не совсем понятна суть называемых авторами «террористических целей».

В.П. Емельянов²¹, Л.А. Моджорян²² под терроризмом понимают активные действия. В.Е. Петрищев²³, А.А. Лунёв²⁴ характеризуют терроризм как «систематическое ... использование насилия...»²⁵. Подобным образом – в самом широком смысле этого слова – трактует терроризм и В.С. Комиссаров

¹⁶ Введение Закона о терроризме 2006 // TheterrorismAct 2006 [Электронный ресурс]. URL: <https://www.gov.uk/government/publications/the-terrorism-act-2006> (дата обращения: 15.03.2016).

¹⁷ См.: Власихин В. А. Закон США о борьбе с терроризмом // Терроризм. Правовые аспекты противодействия: нормативные и международные правовые акты с комментариями, научные статьи / под ред. И.Л. Трунова и Ю.С. Горбунова. Изд. 2-е, перераб. и доп. М.: Эксмо, 2007. С. 456-457.

¹⁸ См.: Федорцев В.А. Негосударственный терроризм как форма политической борьбы: основные признаки и тенденции исторического развития: дис. ... канд. политич. наук. РУДН. М., 2007. С. 19.

¹⁹ См.: Вершинин М. Психологические особенности членов деструктивных и террористических (радикальных) групп [Электронный ресурс]. URL: <http://www.follow.ru/article/339> (дата обращения: 16.04.2016).

²⁰ См.: Гриб Н.Н. Криминологические аспекты противодействия терроризму в современной России: автореф. дис. ... канд. юрид. наук. СПб. 2005. С. 8.

²¹ См.: Емельянов В.П. Терроризм как явление и как состав преступления. Харьков: Право, 1999. С. 28.

²² См.: Моджорян Л.А. Терроризм: правда и вымысел. М.: Юридическая литература, 1983. С. 28.

²³ См.: Петрищев В.Е. Заметки о терроризме. М.: Эдиториал УРСС, 2001. С. 11.

²⁴ См.: Лунёв А.А. Терроризм как объект криминологического изучения: дис. ... канд. юрид. наук. Ростов-на-Дону, 2004. С. 8.

²⁵ Цит. по: Авдеев Ю.И. Терроризм как социально-политическое явление. См.: Современный терроризм: состояние и перспективы / В.Е. Петрищев, Ю.И. Авдеев, О.М. Хлобустов [и др.] / под ред. Е.И. Степанова. М.: Эдиториал УРСС, 2000. С. 37.

– как «применение насилия»²⁶. Н.Б. Крылов и Ю.А. Решетов определяют терроризм как акты насилия²⁷.

Помимо названных точек зрения, в доктрине сложились и иные, раскрывающие понятие терроризма как социально-правового²⁸; социально-политического²⁹ или социальное явление³⁰.

В этой связи интересна точка зрения, определяющая терроризм как социально-политический процесс, что оправдано некоторыми немаловажными обстоятельствами. Терроризм, будучи сложным, многоплановым, изменчивым явлением, сопровождает общественное развитие на протяжении нескольких столетий. Современный же терроризм является частью организованной преступности³¹.

Терроризм – не статичное явление; он всегда коррелирует с изменениями, которые происходят в обществе (в области вооружения, технического и информационного оснащения и т.д.). В связи с этим терроризм существует в соотношении с процессами, которые происходят в различных сферах жизни общества и государства. Сказанное позволяет нам обратиться к имеющимся исследованиям в области определения сущности и содержания преступности.

Так, Ю.И. Бытко, соглашаясь в этом плане с позицией А.Н. Трайнина, В.Н. Кудрявцева, Б.Д. Овчинникова, выделяет в качестве сущностных признаков преступности изменчивость, историческую предопределенность,

²⁶ См.: Комиссаров В.С. Терроризм, бандитизм, захват заложника и другие тяжкие преступления против безопасности общества. По поводу УК РФ. М.: «Кросна-Лекс». 1997. С. 10.

²⁷ См.: Крылов Н.Б., Решетов Ю.А. Государственный терроризм – угроза международной безопасности // Советское государство и право. 1987. № 2. С. 78.

²⁸ См.: Белявский Д.Г. Детерминанты терроризма как социально-правового явления: автореф. канд. ... юрид. наук. М., 2007. С. 7; Дерюгина Ю.Н. Терроризм: уголовно-правовой и криминологический аспекты: дис. ... канд. юрид. наук. М., 2001. С. 47.

²⁹ См.: Лазарев Н.Я. Терроризм как социально-политическое явление: истоки, формы и динамика развития в современных условиях: автореф. дис. ... канд. политич. наук. М., 2007. С. 12-13; Бахтеева А.Р. Политический терроризм как социальное явление современности: автореф. дис. ... канд. социолог. наук. М., 2010. С. 8; Гилинский Я.И. Криминология: теория, история, эмпирическая база, социальный контроль. СПб.: Алеф-Пресс, 2014. С. 282.

³⁰ См.: Резяпова Г.Ф. Терроризм как социальное явление: автореф. дис. ... канд. филос. наук. Уфа, 2005. С. 6; Никитин А.В. Терроризм как форма девиантного поведения (криминологический аспект): автореф. дис. ... канд. юрид. наук. СПб., 2003. С. 7.

³¹ См.: Григорьев А.А. Указ. соч. С. 21; Лунеев В.В. Терроризм и организованная преступность: национальные и транснациональные аспекты // Организованная преступность, терроризм и коррупция: Криминологический ежеквартальный альманах. 2003. № 2. С. 29.

возможность существования только в классовом обществе и подчеркивает тем самым, что это явление динамичное³². Полагаем, что терроризм, как явление обладает такими признаками (изменчивостью, динамичностью, историей существования в обществе), на основе которых можно по аналогии с понятием преступности охарактеризовать его как процесс. При этом, понятие «терроризм» имеет неизменное ядро, состоящее из тех его признаков, которые существуют вне зависимости от происходящих изменений.

Безусловно, все разработки исследователей в области политологии, социологии, философии, криминологии следует признать важными, поскольку они позволяют углубиться в причины возникновения явления терроризма, определения его сущности. Однако подобные трактовки понимания терроризма невозможно использовать в качестве законодательно закреплённого определения, поскольку в настоящее время оно выступает основой для уголовно-правового противодействия террористическим угрозам: более чем в 10 статьях УК РФ устанавливается ответственность за преступления террористической направленности.

Формирование российского законодательства в сфере противодействия терроризму осуществляется на протяжении нескольких десятилетий. За это время оно претерпевало множество изменений. В.С. Комиссаров в своих исследованиях очень подробно анализирует все этапы становления антитеррористического законодательства в России³³.

³² См.: Бытко Ю.И. Преступление и преступность: лекция. Саратов: Изд-во СГАП, 1999. С. 44-45.

³³ Первоначальный этап (70-е годы 20 века) напрямую был связан с развитием международного уголовного права, что послужило криминализации некоторых общественно опасных деяний, являющихся на сегодняшний день преступлениями террористической направленности. Второй этап В.С. Комиссаров связывает с принятием УК РФ 1996 года, где в главе 24 были сосредоточены пять статей, устанавливающие ответственность за преступления террористической направленности. Третий этап связан с формированием фундаментальной базы противодействия терроризму в РФ – специализированного законодательства. Четвертый этап связан с активным развитием международного законодательства в сфере противодействия террористическим угрозам, что обусловило увеличение числа составов преступлений террористической направленности в УК РФ. См.: Комиссаров В.С. Развитие законодательства об ответственности за терроризм в Российской Федерации // Противодействие современной преступности: оценка эффективности уголовной политики и качества уголовного закона: сб. науч. тр. / под ред. Н.А. Лопашенко. Саратов, Саратовский Центр по исследованию проблем организованной преступности и коррупции: Сателлит, 2010. С. 269.

Следует заметить, что в российском законодательстве некоторое время преступное деяние, отражающее сущность современного состава преступления (террористический акт) было известно как терроризм. И только после внесения изменений в УК РФ Федеральным законом от 27.07.2006 № 153-ФЗ терроризм как название статьи Особенной части был «переименован» в террористический акт.

В том числе по этой причине до настоящего времени ведутся дискуссии об удачности использования терминов «терроризм» и «террористический акт», об определении их сущности и статуса в качестве уголовно-правового или криминологического понятий.

Ранее действующий на территории Российской Федерации Федеральный закон «О борьбе с терроризмом» раскрывал сущность терроризма через перечисление возможных общественно опасных деяний, в чем прослеживалось стремление к учету многолетнего опыта международного сообщества³⁴. Полагаем, что такой подход оказался непродуктивным, поскольку невозможно было выявить сущностные признаки терроризма.

В значительной мере этот недостаток был ликвидирован Федеральным законом Российской Федерации № 35-ФЗ «О противодействии терроризму»³⁵ (далее – Федеральный закон РФ № 35-ФЗ), в котором «терроризм» раскрывается как общее, родовое понятие, что является положительным моментом³⁶, поскольку позволяет разграничивать его с такими понятиями как «террористическая деятельность» и «преступления террористической направленности», в том числе с понятием «террористический акт», которым обозначено одно из преступлений террористической направленности,

³⁴ См.: Федеральный закон от 25.07.1998 № 130-ФЗ «О борьбе с терроризмом» // СЗ РФ. 1998. № 31, ст. 3808.

³⁵ См.: Федеральный закон от 06.03.2006 № 35-ФЗ (с изм. и доп. от 06.07.2016, № 374-ФЗ) «О противодействии терроризму» // СЗ РФ. 2006. № 11, ст. 1146; 2016. № 28, ст. 4558.

³⁶ По мнению А.В. Мардояна, стремление к конкретизированному понятию заслуживает положительной оценки. См.: Мардоян А.В. Терроризм как международное преступление: дис. ... канд. юрид. наук. М., 2007. С. 46.

предусмотренное ст. 205 УК РФ. Однако по-прежнему в доктрине преобладает мнение о несовершенстве его сущностного содержания.

В соответствии со ст. 3 Федерального закона РФ № 35-ФЗ терроризм – это идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий.

Данное понятие, наряду с другими (такими как, террористическая деятельность, контртеррористическая операция и т.д.), а также иные положения Федерального закона РФ № 35-ФЗ стали фундаментом для формирования системы мер противодействия терроризму. Однако следует согласиться с мнением В.С. Комиссарова о том, что предложенное в законе понятие характеризует терроризм как социальное явление, затрудняя возможность включения его в механизм уголовно-правового регулирования³⁷.

Среди разработанных на сегодняшний день исследователями понятий терроризма наблюдается тенденция выделения таких его признаков, как насилие, устрашение, воздействие и специальная цель³⁸.

Изучение насилия как социально-правовой категории находит свое отражение в трудах ученых философов, социологов, правоведов. В самом широком смысле насилие понимается как подавление человека не только физически, но и экономически, политически, психологически.

На сегодняшний день насилие является криминообразующим признаком многих составов преступлений, закрепленных в УК РФ.

³⁷ См.: Комиссаров В.С. Террористический акт: уголовно-правовая характеристика основного состава // Терроризм и экстремизм в России и странах АРТ: проблемы правового регулирования и противодействия. Владивосток: Изд-во ДВФУ, 2010. С. 10; Тарбагаев А.Н. Проблемы уголовно-правовой квалификации терроризма // Криминологический журнал Байкальского государственного университета экономики и права. С. 101-106 [Электронный ресурс]. URL: <http://cj.isea.ru/reader/article.asp?id=16519> (дата обращения: 14.03.2016).

³⁸ В этой связи были исследованы понятия терроризма, предложенные А.А. Курбанмагомедовым, А.А. Лунёвым, А.Ю. Никитиным, Д.И. Тисленко, А.А. Григорьевым, В.С. Комиссаровым, В.Е. Петрищевым, Л.А. Маджорян, Ю.М. Антонян и др.

Несмотря на то что понятие терроризма раскрывается не в уголовном законе, а в Федеральном законе РФ № 35-ФЗ, оно может рассматриваться в качестве части механизма уголовно-правового противодействия, поскольку используется при формулировании некоторых диспозиций составов преступлений, предусмотренных гл. 24 УК РФ. Это позволяет рассмотреть понятие насилия, являющегося, по мнению многих авторов, сущностным признаком терроризма, с уголовно-правовой точки зрения³⁹.

Следует заметить, что понятие насилия в действующем законодательстве не закреплено; существуют лишь его определения, разработанные на доктринальном уровне⁴⁰. Несмотря на многообразие таких, многие авторы единодушны в том, что насилие может быть использовано только против человека, животного – живого существа, но не против зданий, сооружений, инфраструктуры, собственности и пр. Причем, в подавляющем большинстве случаев под насилием понимается физическое насилие⁴¹, результатом которого может стать нарушение телесной неприкосновенности, причинение различной тяжести вреда здоровью либо смерти. Психическое насилие как вид уголовно-правового насилия чаще

³⁹ Насилие выделяется в качестве признака терроризма многими авторами, в их числе А.А. Курбанмагомедов, А.А. Лунёв, Д.И. Тисленко, В.Е. Петрищев, Н.Б. Крылов и Ю.А. Решетов, В.С. Комиссаров, Ю.М. Антонян, М.П. Требин, Д.Г. Белявский и др. См.: Тисленко Д.И. Экологический терроризм: уголовно-правовые и криминологические проблемы: дис. ... канд. юрид. наук. Тамбов, 2011. С. 62; Курбанмагомедов А.А. Терроризм на Северном Кавказе (уголовно-правовой и криминологический анализ): дис. ... канд. юрид. наук. Саратов, 2005. С. 8; Лунёв А.А. Указ. соч. С. 8; Петрищев В.Е. Противодействие террористической идеологии – приоритетное направление профилактики терроризма // Материалы II Всероссийской научно-практической Конференции. М.: Университетская книга, 2010. Т. I. С. 75; Крылов Н.Б., Решетов Ю.А. Указ. соч. С. 78; Комиссаров В.С. Терроризм, бандитизм, захват заложника и другие тяжкие преступления против безопасности общества. По поводу УК РФ. М.: Кросна-Лекс, 1997. С. 10; Антонян Ю.М. Криминология. Избранные лекции. М.: Логос, 2004. С. 325; Требин М.П. Терроризм в XXI веке / под общ. ред. А.Е. Тараса. Минск: Харвест, 2003. С. 22; Белявский Д.Г. Указ. соч. С. 7.

⁴⁰ Проблему насилия рассматривали в своих исследованиях такие авторы, как Л.Д. Гаухман, А.А. Пионтковский, Л.В. Сердюк, А.И. Бойцов, Ю.В. Радостева, А.Э. Жалинский и др. См.: Радостева Ю.В. Уголовно-правовое понятие насилия: дис. ... канд. юрид. наук. Екатеринбург, 2006. С. 11; Сердюк Л.В. Насилие: криминологическое и уголовно-правовое исследование / под ред. Щерба С.П. М.: Юрлитинформ, 2002. С. 22; Пионтковский А.А., Меньшагин В.Д. Курс советского уголовного права. Особенная часть. М.: Госюриздат, 1956. Т. 1. С. 722; Бойцов А.И. Понятие насильственного преступления // Криминологические и уголовно-правовые проблемы борьбы с насильственной преступностью. Л., 1988. № 1 (12). С. 138; Жалинский А.Э. Насильственная преступность и уголовная политика // Советское государство и право. 1991. № 3. С. 110; Гаухман Л.Д. Борьба с насильственными посягательствами. М.: Юрид. лит., 1969. С. 3.

⁴¹ См.: Гаухман Л.Д. Указ. соч. С. 3.

всего подразумевается законодателем при характеристике угрозы применения физического насилия⁴².

В уголовном законодательстве терроризм как явление находит свое отражение в первую очередь в совершении террористического акта, при котором создается опасность не только причинения вреда жизни или здоровью людей, но и имущественного ущерба. Соглашаясь с такими исследователями, как М.П. Киреев и С.А. Эфиров⁴³, а также с Д.В. Соповым⁴⁴, полагаем, что терроризм характеризуется не только применением насилия в его узком – уголовно-правовом – понимании. В этой связи интересным представляется понятие терроризма, предложенное в Методических рекомендациях об организации медико-санитарного обеспечения при террористических актах с использованием опасных химических и отравляющих веществ: «насилие или угроза его применения в отношении физических лиц или организаций, а также уничтожение (повреждение) имущества или угроза уничтожения (повреждения) имущества и других материальных объектов»⁴⁵. Тем самым понятия насилия и уничтожения (повреждения) имущества или угрозы его уничтожения (повреждения) разграничиваются.

Исходя из вышеизложенного полагаем, что применительно к терроризму следует говорить о противоправном воздействии, частью которого выступает уголовно-правовое насилие.

Воздействие – это признак, используемый на сегодняшний день законодателем при раскрытии сущности терроризма («практика воздействия»). Однако в уголовно-правовой науке воздействие чаще всего

⁴² См.: Гаухман Л.Д. Насилие как средство совершения преступления. М.: Юрид. лит., 1974. С. 3.

⁴³ См.: Киреев М.П., Эфиров С.А. Исторические и современные взгляды на природу терроризма // Уголовная политика и проблемы безопасности государства. Труды академии управления МВД России. М., 1998. С. 42.

⁴⁴ См.: Сопов Д.В. Уголовная ответственность за терроризм: проблемы квалификации: дис. ... канд. юрид. наук. М., 2004. С. 49.

⁴⁵ Организация медико-санитарного обеспечения при террористических актах с использованием опасных химических и отравляющих веществ. Методические рекомендации (утв. Минздравом РФ 28.12.2001 № 2510/13132-01-34) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

выделяется как специальная цель при характеристике понятия терроризма⁴⁶. Причем акцент делается на опосредованном характере такого воздействия, обусловленного тем, что вред причиняется одним лицам (физический или имущественный, вред государственной или муниципальной собственности), а воздействие тем самым осуществляется на других⁴⁷. Однако в рамках данного диссертационного исследования, соглашаясь в этом аспекте с предложенным законодателем понятием, полагаем необходимым подразумевать под терроризмом практику воздействия, характеризующуюся определенными особенностями.

Эти особенности в первую очередь проявляются в двойственности объекта воздействия, вытекающей из сути опосредованного характера такого воздействия⁴⁸. В этой связи исследователи предлагают определять такие понятия, как стратегические и тактические объекты воздействия⁴⁹. Законодатель относит к объектам, на которые оказывается давление (стратегическим объектам), органы государственной власти, органы местного самоуправления или международные организации. Однако представляется необходимым расширить перечень таких объектов, соглашаясь с формулировкой, предложенной Д.И. Тисленко, и относить к ним органы власти, органы местного самоуправления, международные организации, социальные группы, юридических лиц и физических лиц⁵⁰.

⁴⁶ Данной позиции придерживаются такие авторы, как Д. И. Тисленко, Ю.Н. Дерюгина и др. См.: Тисленко Д.И. Указ. соч. С. 62; Дерюгина Ю.Н. Указ. соч. С. 10.

⁴⁷ См.: Дикаев С.У. Террор, терроризм и преступления террористического характера (криминологическое и уголовно-правовое исследование). СПб.: Изд-во Юридический центр Пресс, 2006. С. 33; Завидов Б.Д. Ответственность за терроризм и преступления, примыкающие к нему. Научно-практический и аналитический комментарий уголовного законодательства по состоянию на 12 октября 2010 года [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

⁴⁸ Двойственность объектов воздействия при терроризме отмечали также В.И. Василенко, Я.И. Гилинский. См.: Василенко В.И. Международный терроризм в условиях глобального развития: дис. ... д-ра политич. наук. М., 2003. С. 55; Гилинский Я.И. Указ. соч. С. 282.

⁴⁹ См.: Федорцев В.А. Указ. соч. С. 19.

⁵⁰ На необходимость расширения объектов воздействия указывали такие авторы, как Д.И. Тисленко, Ю.Н. Дерюгина, В.П. Емельянов и др. См.: Тисленко Д.И. Указ. соч. С. 46; Дерюгина Ю.Н. Указ. соч. С. 10; Емельянов В.П. Понятие терроризма в уголовном законодательстве России и Украины. Сравнительный анализ // Российская юстиция. 1999. № 11. С. 42.

Помимо названных, одним из существенных признаков терроризма, по мнению многих авторов, является специальная цель⁵¹. Обращает на себя внимание тот факт, что в законодательном определении понятия терроризма какая-либо цель не называется в качестве его существенного признака. Между тем при характеристике состава преступления, предусмотренного ст. 205 УК РФ, цель выделяется как неотъемлемый признак субъективной стороны преступления.

В теории цели, присущие терроризму, классифицируются на публичные и политические⁵²; внушающие страх; заставляющие действовать или воздерживаться от действий в нужном террористам направлении⁵³ и др. Современные исследователи отмечают расширение целей, преследуемых террористами (террористическими организациями или сообществами). Методы (в том числе и насильственные), используемые террористами, могут применяться не только в политических целях (таких как, принуждение субъектов власти к принятию или воздержанию от принятия какого-либо решения), но и быть направленными на изменение отношения населения к власти, какой-либо социальной группе и т.п. Например, целью немецкой организации RAF, как отмечают исследователи, было спровоцировать массовые репрессии и тем самым вызвать открытую конфронтацию властей и населения⁵⁴. Кроме того, акции террористов могут быть направлены на стимулирование массового повстанческого движения или трансформацию иным образом политических взглядов населения или какой-либо социальной группы.

Избегая конкретизации цели, которую могут преследовать террористы, В.Е. Петрищев подчеркивает в предложенном им понятии терроризма, что через устрашение физических лиц осуществляется управление их

⁵¹ К таковым следует отнести А.А. Лунёва, Ю.Н. Дерюгину, В.П. Емельянова, Л.А. Маджорян, Д.Г. Белявского и др.

⁵² См.: Василенко В.И. Указ. соч. С.53.

⁵³ См.: Крылов Н.Б., Решетов Ю.А. Указ. соч. С. 78.

⁵⁴ См.: Федорцев В.А. Указ. соч. С. 20.

поведением в выгодном для террористов направлении⁵⁵. Нет сомнений в том, что терроризм сегодня следует связывать не только с воздействием на различные государственные структуры. Так, председатель Государственной Думы С.Е. Нарышкин в своем выступлении назвал в качестве одной из целей террористов «разрушение самих ценностей цивилизованного мира, культуры и демократических принципов»⁵⁶.

Полагаем, что в выделении специальной цели как признака терроризма нет необходимости. Это обусловлено тем, что практика воздействия является самой сутью терроризма. Цель же, называемая некоторыми авторами как отдельный признак терроризма, в действующем законодательном понятии характеризует объект такого воздействия.

На сегодняшний день специализированное законодательство раскрывает понятие терроризма как идеологию насилия и практику воздействия. Спорным, на наш взгляд, является определение «места» идеологии в понятии терроризма: возможно ли раскрывать данное явление через понятие идеологии.

Известно, что идеология есть система взглядов и идей⁵⁷. Если обратиться к науке этимологии, сущностное значение суффикса «-изм», входящего в состав таких слов русского языка, как «коммунизм», «коллективизм», «терроризм» и др., раскрывается следующим образом: при добавлении к существительному (в интересующем нас примере – это «террор»), он образует существительное мужского рода со значением течения, направления мысли и т.п. («терроризм»)⁵⁸. В связи с этим представляется допустимым раскрывать понятие терроризма через понятие идеологии. Однако необходимо определить место идеологии как основы

⁵⁵ См.: Петрищев В.Е. Указ. соч. С. 75.

⁵⁶ См.: Нарышкин Сергей назвал главные цели террористов [Электронный ресурс]. URL: <http://govoritmoskva.ru/news/59758/> (дата обращения 08.03.2016).

⁵⁷ См.: Ожегов С.И., Шведов Н.Ю. Толковый словарь русского языка. 4-е изд., дополн. М.: Азбуковник, 1999. С. 236.

⁵⁸ Безусловно, использование знаний других наук, в частности гуманитарных, не должно стать единственным основанием для определения сущности правовых понятий. Однако игнорировать особенности словообразования, русского языка нельзя.

терроризма, соглашаясь в этом вопросе с такими исследователями, как Е.В. Петрищев⁵⁹, А.А. Лунёв⁶⁰. Лежащая в основе терроризма система взглядов и идей оправдывает применение насилия и иных противоправных форм воздействия. По мнению Е.П. Ильина, любая идеология (в том числе и та, что может стать основой терроризма) формирует определенную картину мира и мобилизует, то есть предлагает конкретный образ действий⁶¹. Идеологическое обоснование является отличительной чертой воздействия при терроризме, что позволяет отграничивать преступления террористической направленности от иных противоправных деяний, предусмотренных УК РФ.

Особое место среди признаков терроризма, выделяемых доктриной и законодателем, занимает устрашение. Проводя разграничение между терроризмом и уголовной преступностью, В.В. Витюк и С.А. Эфиров отмечают, что террористы стремятся запугать общество, другие же преступники стараются не привлекать к себе внимания⁶². Устрашение – исторически и этимологически обоснованный признак терроризма, поскольку понятие последнего происходит от слова «террор», означающего «страх, ужас».

Как следует из законодательного определения, «место» устрашения в понятии терроризма четко не определено. Некоторые исследователи, такие, как Н.Б. Крылов и Ю.А. Решетов⁶³, выделяют в качестве одной из целей терроризма внушение страха. Социально-психологическое устрашение как одну из целей терроризма определяют Ю.И. Дорожкин и Л.О. Изилиева⁶⁴. Между тем Т.С. Бояр-Созонович подчеркивает, что если и рассматривать устрашение как цель терроризма, то исключительно как опосредованную,

⁵⁹ См.: Петрищев В.Е. Указ. соч. С. 75.

⁶⁰ См.: Лунёв А.А. Указ. соч. С. 8.

⁶¹ См.: Ильин Е.П. Система противодействия идеологии терроризма в Российской Федерации: становление и перспективы развития // Материалы II Всероссийской научно-практической Конференции. М.: Университетская книга, МГУ 13-14 октября 2010 г. Т. I. С. 10.

⁶² См.: Витюк В.В., Эфиров С.А. Указ. соч. С. 229.

⁶³ См.: Крылов Н.Б., Решетов Ю.А. Указ. соч. С. 78.

⁶⁴ См.: Дорожкин Ю.Н., Изилиева Л.О. Современный терроризм: природа, особенности и средства противодействия // Экономика и управление. 2005. № 1. С. 20-21.

промежуточную, поскольку запугивание является средством достижения других, стратегических, целей⁶⁵. А.К. Шарапов полагает, что страх может оцениваться террористами и как цель, и как средство их политической деятельности⁶⁶.

Из сущности законодательного определения понятия терроризма следует, что устрашение является одной из форм противоправных насильственных действий. Также указывается, что насилие и практика воздействия должны быть связаны с устрашением и (*или*) иными формами противоправных насильственных действий. Такое расширительное толкование терроризма и неизвестность правовой природы иных форм противоправных насильственных действий нельзя признать удачным.

Резюмируя вышеизложенное, в качестве сущностных признаков терроризма выделим следующие:

- он представляет собой практику воздействия;
- воздействие является идеологически обоснованным;
- воздействие сопряжено с устрашением населения;
- воздействие имеет опосредованный характер: имущественный, физический и иной вред причиняется одним лицам (тактические объекты), а воздействие осуществляется на других (стратегические объекты).

Терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом.

Российский законодатель в сфере противодействия терроризму оперирует и другими понятиями, такими как террористический акт, террористическая деятельность и преступления террористической

⁶⁵ См.: Бояр-Созонович. Международный терроризм: политико-правовые аспекты. Киев-Одесса: Лыбидь, 1991. С. 214.

⁶⁶ См.: Шарапов А.К. Политический терроризм: развитие ресурсного потенциала и типология: дис. ... канд. политич. наук. Чита, 2005. С 16.

направленности. Соотношение и определение сущности каждого из них способствует более полному раскрытию специфики понятия терроризма, присущего российскому законодательству и праву.

Терроризм как идейно обоснованная практика воздействия является родовым, более широким понятием по отношению к различным формам проявления террористической деятельности⁶⁷. Само по себе явление терроризма находит свою конкретизацию в осуществлении террористической деятельности⁶⁸. Последняя, в свою очередь, характеризуется совершением преступлений террористической направленности, иных запрещенных законом или иными правовыми актами общественно опасных деяний (например, ст. 20.3 КоАП РФ – «пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутик или символик, пропаганда либо публичное демонстрирование которых запрещены федеральными законами»), а также иных деяний (например, обмена сообщениями между террористами). Кроме того, террористический акт, представляющий собой самое опасное проявление терроризма, является одним из преступлений террористической направленности.

На сегодняшний день Федеральный закон РФ № 35-ФЗ раскрывает понятие террористической деятельности через перечисление деяний, которые под нее подпадают. Следует заметить, что подобное понимание террористической деятельности вызывает определенные споры. Как было отмечено ранее, террористы используют новейшие усовершенствования и способы осуществления своей деятельности. Раскрываемое через перечисление конкретных деяний понятие террористической деятельности никогда не сможет своевременно отвечать тем изменениям, которым

⁶⁷ См.: Побегайло Э.Ф. Терроризм и уголовная ответственность // Актуальные проблемы Европы. Проблемы терроризма: Проблемно-тематический сборник. 1997. № 4. С. 203.

⁶⁸ Как известно терроризм является одной из форм проявления экстремизма. Федеральный Закон от 25.07.2002 № 114-ФЗ (с изм. и доп. от 06.07.2016) «О противодействии экстремистской деятельности» признает экстремизм в качестве синонима понятия экстремистская деятельность. Однако Федеральный Закон «О противодействии терроризму» различает понятия «терроризм» и «террористическая деятельность».

подвергаются средства, орудия, способы, методы ее осуществления⁶⁹. Кроме того, использование новых технологий значительно расширяет сферу деятельности террористов.

К террористической деятельности законодателем отнесены следующие деяния:

- организация террористического акта – ч. 4 ст. 205¹ УК РФ;
- финансирование террористического акта – ч. 1 ст. 205¹ УК РФ;
- реализация террористического акта – ст. 205 УК РФ;
- организация незаконного вооруженного формирования и участие в нем для реализации террористического акта – ст. 208 УК РФ;
- организация преступного сообщества (преступной организации) и участие в нем (ней) для реализации террористического акта – ст. 210 УК РФ;
- организация организованной группы и участие в ней для реализации террористического акта. УК РФ не предусматривает ответственность за совершение подобного преступления. Совершение террористического акта в составе организованной группы необходимо квалифицировать по п. «а» ч. 2 ст. 205 УК РФ. За организацию совершения террористического акта устанавливается ответственность в ч. 4 ст. 205¹ УК РФ;
- вербовка, вооружение – ч. 1 ст. 205¹ УК РФ;
- пособничество – ч. 3 ст. 205¹ УК РФ;
- распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности (иными словами, пропаганда указанных материалов и информации) – частично данные действия нашли свое отражение в ст. 205² УК РФ. Однако данная статья охватывает только случаи распространения такой информации публично, не позволяя квалифицировать по ст. 205² УК РФ иные деяния,

⁶⁹ См.: Шевченко И.В. Уголовная ответственность за террористическую деятельность: уголовно-правовой и правоприменительный аспекты: дис. ... канд. юрид. наук. Тамбов, 2010. С. 36.

связанные с распространением флеш-накопителей, компакт-дисков, печатной продукции без признака публичности.

- обучение – ч. 1 ст. 205¹ УК РФ. В данной статье говорится не об обучении, а о подготовке лица в целях совершения указанных в диспозиции преступлений. Пленум Верховного суда по этому вопросу разъясняет, что подготовка и есть обучение различным правилам обращения с оружием, боеприпасами и так далее⁷⁰;

- планирование и подготовка террористического акта. Уголовный закон не содержит подобного деяния. Представляется возможным отнести их к организации террористического акта. Постановление Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» (далее – Постановление Пленума ВС РФ от 09.02.2012 № 12) не разъясняет, что подразумевается под организацией террористического акта. Однако по аналогии с понятиями, отражающими сущность других деяний, можно согласиться с отнесением к организации террористического акта его планирования и подготовки. Так сущность организации вооруженного мятежа может выражаться в разработке плана вооруженного выступления, подготовке программных документов⁷¹; в подготовке и создании условий, обеспечивающих его проведение⁷².

- подстрекательство к террористическому акту. Состав такого преступления в главе 24 Особенной части УК РФ отсутствует. Однако, в соответствии со статьями 33, 34, 67 УК РФ возможно привлечение к уголовной ответственности таких подстрекателей. Частные случаи ответственности за подстрекательство предусмотрены статьями 205¹ и 205² УК РФ;

⁷⁰ См.: Постановление Пленума Верховного суда Российской Федерации от 09.02.2012 № 12 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // Рос. газета. 2012. 17 фев.

⁷¹ См.: Преступления против основ конституционного строя и безопасности государства: учебное пособие / под ред. А.П. Кузнецова. Н. Новгород: Нижегородская правовая академия, 2006. С. 31.

⁷² См.: Курс уголовного права. Т. 5 / под ред. Борзенкова Г.Н., Комиссарова В.С. М.: Зерцало, 2002. С. 305.

- пропаганда идей терроризма. УК РФ не предусматривает ответственности за подобное деяние. Между тем ст. 20.3 КоАП РФ устанавливает ответственность за пропаганду либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутик или символов, пропаганда либо публичное демонстрирование которых запрещены федеральными законами. Итак, если иметь в виду, что терроризм является крайней формой проявления экстремизма, то теоретически возможно привлечение к административной ответственности за пропаганду символики и атрибутики какой-либо террористической организации (сообщества). Однако предварительно необходимо получить решение суда о признании какой-либо организации (сообщества) в качестве террористической (ого);

- использование террористов. Не совсем понятна сущность указанных действий. По всей видимости, подразумевается использование террористов государственными и иными субъектами в политических целях⁷³. Между тем ни УК РФ, ни иные нормативно-правовые акты не устанавливают ответственность за подобное деяние.

Помимо вышеназванных деяний, которые согласно Федеральному закону РФ № 35-ФЗ входят в понятие террористической деятельности, УК РФ содержит и иные, которые можно отнести к ней. Например, не совсем понятно, почему вышеназванный закон не относит к террористической деятельности совершение таких преступлений, как: организация террористического сообщества и участие в нем; организация деятельности террористической организации и участие в деятельности такой организации. Полагаем, что это может быть связано с неприведением в соответствие положений УК РФ с нормами Федерального закона РФ № 35-ФЗ.

⁷³ В. Путин в интервью телеканалу «Россия 1» говорил: «Использование террористов для решения каких-то политических задач – опасно». См.: Путин предупреждал США, что нельзя прибегать к помощи террористов [Электронный ресурс]. URL: <http://www.kp.ru/online/news/2040147/> (дата обращения: 24.05.2015).

Однако само по себе понятие террористической деятельности изначально не отвечает требованиям юридической техники, поскольку не позволяет выявить существенные признаки данного явления и относить какую-либо деятельность к террористической.

Проблема определения содержания термина «террористическая деятельность» осложняется при анализе норм УК РФ. В значительной мере существующие недостатки уже были исследованы в работах П.В. Агапова, Н.А. Егоровой, К.В. Михайлова, Б.В. Сидорова и др.⁷⁴. Между тем последние изменения в УК РФ, внесенные Федеральным законом РФ от 06.07.2016 № 375-ФЗ, частично устранили имеющиеся пробелы, вызвав, в свою очередь, новые вопросы⁷⁵.

Понятие террористической деятельности используется законодателем при формировании диспозиций статей 205¹, 205², 205³, 205⁴ и 211 УК РФ, а также примечаний к статьям 205², 205³ УК РФ.

Статья 205¹ УК РФ устанавливает ответственность за содействие террористической деятельности. При этом диспозиция части 1 данной статьи раскрывает содержание понятия террористической деятельности посредством перечисления деяний, предусмотренных УК РФ в качестве преступлений. К ним отнесены: ст. 205, 205², 205³, 205⁴, 205⁵, 206, 208, 211, 220, 221, 277, 278, 279, 360 и 361 УК РФ⁷⁶. Из названных только деяния,

⁷⁴ См.: Агапов П.В., Михайлов К.В. Уголовная ответственность за содействие террористической деятельности: тенденции современной уголовной политики. Саратов: Изд-во Саратов. юрид. ин-та МВД России, 2007. С. 144 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс»; Сидоров Б.В. Терроризм и террористическая деятельность: вопросы соотношения, системный анализ и проблема совершенствования уголовно-правового и криминологического противодействия // Вестник экономики, права и социологии. 2015, № 4. С. 234-243; Егорова Н.А. Противодействие терроризму: новеллы уголовного законодательства // Криминологический журнал Байкальского государственного университета экономики и права. 2014. № 3. С. 127-134.

⁷⁵ См.: Федеральный закон Российской Федерации от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный Кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СЗ РФ. 2016. № 28, ст. 4559.

⁷⁶ Здесь и далее в тексте, касающемся определения понятия террористической деятельности, *курсивом* будут выделены те статьи УК РФ, которыми были дополнены диспозиции исследуемых статей. Помимо расширения перечня деяний, которыми обозначается понятие террористической деятельности в ч. 1 ст. 205¹ УК РФ, он был дополнен новой, ранее неизвестной нормой, – ст. 361 УК РФ («акт международного терроризма»). По-прежнему не предусматривается по ч. 1 ст. 205¹ УК РФ ответственность за склонение, вербовку или иное вовлечение лица в финансирование терроризма. Привлечение к уголовной

предусмотренные статьями 205, 205² (частично) и 208 относятся Федеральным закон РФ № 35-ФЗ к понятию террористической деятельности. Остальные же деяния, предусмотренные статьями 205³, 205⁴, 205⁵, 206, 211, 220, 221, 277, 278, 279, 360 и 361 УК РФ, в соответствии с вышеназванным законом к террористической деятельности не относятся.

В свою очередь примечание к ст. 205¹ УК РФ в части определения понятия финансирования терроризма не предусматривает возможность оказания финансовых услуг для организации, подготовки или совершения преступления, предусмотренного ст. 361 УК РФ («акт международного терроризма»), что обусловлено установлением самостоятельной ответственности за подобные деяния по ч. 2 ст. 361 УК РФ. Нет сомнений в том, что такое законодательное решение требует изучения на уровне самостоятельного исследования. Однако следует отметить, что наказание за финансирование актов международного терроризма (ч. 2 ст. 361 УК РФ) аналогично наказанию за финансирование терроризма по ч. 1 ст. 205¹ УК РФ. Более того, определенные сомнения вызывает законодательное конструирование ст. 361 УК РФ, где наказание за деяния, предусмотренные ч. 1 ст. 361 УК РФ значительно превышает наказание за деяния, предусмотренные частью 2 этой же статьи. Исходя из вышеизложенного, квалифицированный состав ч. 2 ст. 361 УК РФ не является таковым по своему содержанию. Целесообразным, на наш взгляд, было бы исключить (декриминализовать) ч. 2 ст. 361 УК РФ и дополнить перечень преступлений, предусмотренный Примечанием 1 к ст. 205¹ УК РФ, ст. 361 УК РФ.

Статья 205³ УК РФ устанавливает ответственность за прохождение обучения в целях осуществления террористической деятельности. При этом диспозиция данной статьи в качестве цели обучения называет либо осуществление террористической деятельности, либо совершение одного из следующих преступлений: 205¹, 206, 208, 211, 277, 278, 279, 360 и 361

ответственности за данное деяние возможно лишь на основе норм Общей части – как приготовление к преступлению.

УК РФ. Однако деяния, предусмотренные статьями 205¹, 208 УК РФ, согласно Федеральному закону РФ № 35-ФЗ, входят в понятие террористической деятельности. Между тем отсутствие в перечне указанного в диспозиции ст. 205³ УК РФ состава преступления, предусмотренного ст. 205 УК РФ, нелогично. Приблизительно такая же проблема выявляется при анализе диспозиции ч. 1 ст. 205⁴ УК РФ, в которой устанавливается ответственность за создание террористического сообщества в целях осуществления террористической деятельности либо для подготовки или совершения одного либо нескольких преступлений, предусмотренных статьями 205¹, 205², 206, 208, 211, 220, 221, 277, 278, 279, 360 и 361 УК РФ.

До вступивших в законную силу изменений неизвестным оставалось содержание понятия террористической деятельности, предусмотренного частями 1 и 2 ст. 205² УК РФ. Данный недостаток был устранен путем включения Примечания 2 к ст. 205² УК РФ следующего содержания: в настоящей статье под террористической деятельностью понимается совершение хотя бы одного из преступлений, предусмотренных статьями 205-206, 208, 211, 220, 221, 277, 278, 279, 360 и 361 настоящего Кодекса. Если проводить сравнение данной нормы с положениями Федерального закона РФ № 35-ФЗ, можно установить, что ст. 205³, 205⁴, 205⁵, 205⁶, 206, 211, 220, 221, 277, 278, 279, 360 и 361 не используются названным Федеральным законом для раскрытия содержания понятия террористической деятельности. Более того, исходя из сущностного содержания Примечания 2 ст. 205² УК РФ к террористической деятельности относится также деяние, предусмотренное ст. 205⁶ УК РФ («несообщение о преступлении»)⁷⁷, являющееся по своей природе одним из видов прикосновенности к преступлению⁷⁸. Соглашаясь с

⁷⁷ В криминализации подобного деяния видится заимствование опыта уголовного законодательства Республики Узбекистан, где подобная статья (ст. 155¹) была введена Законом Республики Узбекистана от 20.01.2014 года № ЗРУ-365. См.: Уголовный кодекс Республики Узбекистан [Электронный ресурс]. URL: http://www.lex.uz/pages/getact.aspx?act_id=111457 (дата обращения: 07.04.2016).

⁷⁸ Проблема установления уголовной ответственности за недоносительство уже уделялось внимание на уровне самостоятельных исследований. См.: Лапунин М.М. Уголовная ответственность за недоносительство: история и современность // Сб. науч. тр. под ред. Н.А. Лопашенко. Саратов: Сателлит, 2006 [Электронный ресурс]. URL: [http://sartracc.ru/i.php?filename=Pub/lapunin\(09-00-07\).htm&oper=read_file](http://sartracc.ru/i.php?filename=Pub/lapunin(09-00-07).htm&oper=read_file) (дата обращения: 04.07.2016); Солопанов Ю.В. Об ответственности за недонесение о готовящемся или

такими исследователями, как М.М. Лапунин и Ю.В. Солопанов полагаем чрезмерной установление уголовной ответственности за недоносительство, что свидетельствует не о всестороннем предупреждении совершения преступлений террористической направленности, а о бессилии правоохранительных органов в борьбе с крайне опасным явлением терроризма.

Кроме того, ч. 4 ст. 211 УК РФ, содержащая в диспозиции понятие террористической деятельности, его не раскрывает. Возникает вопрос, как трактовать данное понятие: с учетом положений Федерального закона РФ № 35-ФЗ либо положений УК РФ (по аналогии с другими статьями)⁷⁹.

Как следует из проведенного анализа, понятие террористической деятельности раскрывается в том числе через перечисление конкретных составов преступлений, именуемых в доктрине и правоприменении преступлениями террористической направленности⁸⁰. Перечень таких преступлений закреплен на сегодняшний день не только в Федеральном законе РФ № 35-ФЗ и в УК РФ, но и в Указании Генпрокуратуры России № 65/11, МВД России № 1 от 01.02.2016 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности», где в качестве террористических названы преступления, предусмотренные статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, 211 ч. 4, 277, 360, а также статьи 220, 221, 278, 279, 282¹, 282² УК

совершенном преступлении [Электронный ресурс]. URL: <http://law.edu.ru/article/article.asp?articleID=158462> (дата обращения: 04.07.2016).

⁷⁹ Федеральным законом РФ от 05.05.2014 № 130-ФЗ была введена ч. 3 ст. 64 УК РФ, предусматривающая ограничения применения ч. 1 ст. 64 УК РФ о назначении более мягкого наказания, связанные с совершением виновным преступлений, предусмотренных статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, частями 3, 4 ст. 206, ч. 4 ст. 211 (Федеральным законом РФ от 06.07.2016 № 375-ФЗ данный перечень был дополнен ст. 361 УК РФ), а также в совершении сопряженных с осуществлением террористической деятельности преступлений, предусмотренных статьями 277, 278, 279 и 360 УК РФ. Предложенный перечень преступлений также свидетельствует о неединообразном понимании террористической деятельности в УК РФ.

⁸⁰ Постановление Пленума Верховного Суда РФ № 12-ФЗ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» разъясняет ряд положений статей 205, 205¹, 205², 208 УК РФ и вопросы их квалификации, а также называет перечень преступлений, ответственность за которые устанавливается УК РФ в целях уголовно-правового обеспечения противодействия терроризму и выполнения международных обязательств: статьи 205, 205¹, 205², 206, 208, 211, 220, 221, 227, 277, 278, 279, 360. Анализ содержания данного Постановления Пленума ВС РФ позволяет сделать вывод о том, что те деяния, которые составляют понятие террористической деятельности, и являются преступлениями террористической направленности.

РФ. Кроме того, статьи 206, 209, 210, 281, 295, 317, 318 УК РФ могут признаваться преступлениями террористической направленности при наличии в статистической карточке отметки о связи совершенных преступлений с террористической деятельностью⁸¹. Безусловное признание в качестве террористических преступлений, предусмотренных статьями 282¹ и 282² УК РФ, является, на наш взгляд, спорным; представляется необходимым определить их в группу преступлений, признаваемых в качестве террористических при наличии соответствующей отметки об этом в статистической карточке⁸².

Такая позиция обусловлена следующим: статьи 282¹ и 282² УК РФ тем же Указанием Генпрокуратуры России № 65/11 отнесены к преступлениям экстремистской направленности, что оправдано, учитывая специфику данных деяний. Следует также заметить, что ни один из составов преступлений, предусмотренных статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, 211 ч.4, 277, 360 УК РФ не определен в качестве преступления экстремистской направленности, хотя именно террористическая деятельность является высшей формой проявления экстремизма. Терроризм, террористическая деятельность и преступления террористической направленности обладают рядом отличительных признаков. Кроме того, за создание террористического сообщества и организации установлены специальные составы преступлений, предусмотренные ст. 205⁴ и 205⁵ УК РФ. В случае же совершения участником экстремистского сообщества (организации) или организатором конкретного преступления его действия следует квалифицировать по

⁸¹ См.: Указание Генпрокуратуры России N 65/11, МВД России N 1 от 01.02.2016 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

⁸² Спорным также является нахождение в перечне преступлений террористической направленности статей 220 и 221 УК РФ. Однако данная позиция может быть оправдана принятием Генеральной Ассамблеей ООН разработанной по инициативе РФ Международной конвенции о борьбе с актами ядерного терроризма в 2005 году.

совокупности преступлений⁸³, что, как видится, касается и совершения преступлений террористической направленности⁸⁴.

Таким образом, согласно Указанию Генпрокуратуры России № 65/11 собственно террористической признается деятельность, связанная с совершением преступлений, предусмотренных статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, 211 ч.4, 277, 360, а также статьями 220, 221, 278, 279, 282¹, 282² УК РФ. Вышеизложенное свидетельствует о неединообразном понимании сущности деяний, являющихся преступлениями террористической направленности, а соответственно, и террористической деятельности, что не только затрудняет правовую оценку данных понятий, но и анализ и учет состояния преступности террористической направленности.

Представляется, что в самом широком смысле террористическую деятельность следует рассматривать как деятельность, связанную не только с совершением преступлений, но и административных правонарушений (например, ч. 6 ст. 13.15 КоАП РФ). Подобная деятельность может также носить формально правомерный характер (например, создание благотворительных организаций в целях финансирования террористической деятельности⁸⁵).

Таким образом, террористическая деятельность представляет собой деятельность, которая устанавливается УК РФ и КоАП РФ в качестве запрещенной.

На сегодняшний день приходится констатировать факт несовершенства действующего законодательства в сфере противодействия террористическим угрозам в части определения сущности террористической деятельности.

⁸³ См.: Постановление Пленума Верховного Суда Российской Федерации от 28.06.2011 № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // Рос. газета. 2011. 04 июля.

⁸⁴ Федеральным законом от 05.05.2014 № 128-ФЗ была введена ст. 354¹ («реабилитация нацизма»), в отношении которой не было определенности в отнесении ее к террористическим или экстремистским преступлениям до вступления в силу Указания Генпрокуратуры России № 64/11. Данным указанием ст. 354¹ была отнесена к преступлениям экстремистской направленности.

⁸⁵ На протяжении уже многих лет использование некоммерческого сектора для финансирования терроризма представляет серьезную опасность. См.: Проект по изучению рисков, связанных с деятельностью благотворительных организаций [Электронный ресурс]. URL: http://www.un.org/ru/terrorism/ctif/proj_charities.shtml (дата обращения 13.03.2016).

Наличие данной проблемы не позволяет эффективно регулировать общественные отношения и формировать профилактические меры противодействия терроризму и различным формам его проявления. Исследователи отмечают, что только единство юридической терминологии во всей системе российского права может способствовать адекватной реализации принципа законности⁸⁶. Однако даже сформулированное как общеправовое понятие «террористическая деятельность» все равно будет требовать конкретизации в УК РФ, поскольку она выражается в совершении не только преступлений, но и в некоторых административных правонарушениях.

В этой связи представляется необходимым проанализировать уже существующие в доктрине понятия террористической и экстремистской деятельности⁸⁷ в целях выделения на их основе признаков и формулирования соответствующего общеправового понятия террористической деятельности.

По мнению А.Г. Хлебушкина, одним из признаков экстремистской деятельности выступает *деятельный характер*⁸⁸. Полагаем, что данный признак в равной степени может характеризовать и террористическую деятельность. Деятельный характер означает, что в правовом понимании террористическая деятельность – это только акты человеческого поведения.

Кроме того, при характеристике экстремистской деятельности А.Г. Хлебушкин также выделяет такой ее признак, как *противоправность*⁸⁹. Аналогично данный признак может и должен отражать сущность террористической деятельности. Противоправность означает, что данная деятельность запрещена законом, а именно – УК РФ и (или) КоАП РФ.

⁸⁶ См.: Фомина Л.Ю. Обеспечение единства терминологии нормативных правовых актов: проблемы и перспективы // Социально-политические науки. 2012. № 1. С. 96; Гордеев Н.С. Реализация принципа законности при противодействии экстремизму: теоретические и практические проблемы // Ученые записки Тамбовского отделения Рос МУ. 2016. № 5. С. 75.

⁸⁷ Возможность исследования понятия экстремистской деятельности обусловлена законодательным подходом отнесения террористической деятельности к экстремистской.

⁸⁸ См.: Хлебушкин А.Г. Преступления экстремистской направленности в системе посягательств на основы конституционного строя Российской Федерации. Вопросы квалификации и судебной практика / под ред. Н.А. Лопашенко. М.: Проспект, 2015. С. 29.

⁸⁹ См.: Хлебушкин А.Г. Указ. соч. С. 30.

Специальным и присущим исключительно террористической деятельности как высшей форме проявления деятельности экстремистской исследователями называется такой ее признак, как *цель*. И.В. Шевченко признает в качестве таковой воздействие на принятие решения органом государственной власти, органом местного самоуправления или международной организации⁹⁰. Без соответствующей конкретизации на террористические цели как сущностный признак террористической деятельности указывает и В.П. Кашепов⁹¹. Как видится, данный признак террористической деятельности оперирует к понятию терроризма, в котором специальная цель является, по мнению названных авторов, сущностным признаком. Однако, учитывая предложенное диссертантом понятие терроризма, где цель не называется в качестве сущностного признака, представляется невозможным использовать его при раскрытии понятия террористической деятельности.

Следует также обратить внимание на такой признак террористической деятельности, как *выраженность ее в совершении преступлений или правонарушений террористической направленности*⁹². Так или иначе, этот признак находит свое отражение в определениях, предложенных И.В. Шевченко, В.П. Кашеповым, Н. Семькиным⁹³, Н.А. Егоровой. Как отмечает В.В. Лунеев преступления террористической направленности есть конкретные формы террористической деятельности⁹⁴. Однако названные исследователи связывают террористическую деятельность исключительно с преступными деяниями.

⁹⁰ См.: Шевченко И.В. Указ. соч. С. 37.

⁹¹ См.: Кашепов В.П. Уголовно-правовое регулирование противодействия терроризму // Уголовное право. 2006. № 3. С. 35.

⁹² Проводя аналогию с понятием «преступная деятельность», под которой понимается система взаимосвязанных преступных деяний, террористическую деятельность необходимо понимать как совершение не одного, а нескольких преступлений (правонарушений) террористической направленности. См.: Криминология: учебник для вузов / под общ. ред. А.И. Долговой. М.: Норма, 2005. С. 67.

⁹³ См.: Семькин Н. Создание террористических групп необходимо криминализовать в УК всех государств Содружества // Российская юстиция. 2003. № 1. С. 66.

⁹⁴ См.: Лунеев В.В. Преступность XX века: мировые, региональные и российские тенденции. М.: Волтерс Клувер, 2005. С. 634.

Между тем представляется необходимым понимать террористическую деятельность не только как совершение конкретных преступлений, но и административных правонарушений, что обусловлено в первую очередь невозможностью привлечения к уголовной ответственности юридических лиц.

На основе вышеизложенного, а также имеющихся исследований на тему организованной преступной деятельности⁹⁵, террористическую деятельность следует определять с точки зрения трех подходов.

Первый – характеризует террористическую деятельность как деятельность, выражающуюся не только в совершении преступлений или правонарушений террористической направленности, но и других деяний, связанных с ее организационным, информационным, идеологическим и иным обеспечением, и не являющихся преступлениями (правонарушениями).

Второй подход определяет террористическую деятельность как запрещенную Уголовным Кодексом РФ и (или) Кодексом РФ об административных правонарушениях деятельность, выражающуюся в совершении деяний террористической направленности. Данное понятие является общеправовым, созданным для целей разработки и повышения эффективности уже существующих мер противодействия терроризму, которое следует закрепить в ст. 3 Федерального закона № 35-ФЗ.

Третий подход представляет понятие террористической деятельности в ее самом узком, уголовно-правовом смысле, что связано с необходимостью конкретизации данного понятия на уровне Уголовного закона. В связи с этим, а также для целей недвусмысленного понимания террористической деятельности в контексте некоторых составов преступлений, предусмотренных главой 24 УК РФ, в Примечании 1.2 к ст. 205¹ («содействие террористической деятельности»), необходимо закрепить следующее понятие: «Под террористической деятельностью в статьях

⁹⁵ См.: Борьба с криминальными рынками в России / под общ. ред. В.В. Меркурьева. М.: Проспект, 2015. С. 115.

настоящего Кодекса следует понимать совершение хотя бы одного из преступлений, предусмотренных статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, 211 ч. 4, статьями 220, 221, 277, 278, 279, 360, 361, а также статьями 206, 209, 210, 220, 221, 281, 295, 317, 318 настоящего Кодекса, 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».

Понятие преступлений террористической направленности также подвергалось анализу на уровне доктрины. В числе признаков авторами называются специальная цель (по аналогии с понятием «террористическая деятельность»)⁹⁶, устрашение (представляется, что данный признак в большей степени характерен для терроризма, нежели чем для преступлений террористической направленности), особенности субъективной стороны преступления (в виде прямого умысла) и другие⁹⁷.

Между тем, по нашему мнению, следует говорить не только о преступлениях, но и правонарушениях террористической направленности, поскольку террористическая деятельность проявляется не только в совершении отдельных преступлений. Как общеправовой закон, имеющий широкую сферу действия, Федеральный закон РФ № 35-ФЗ должен содержать понятие преступлений (*правонарушений*) террористической направленности, к которым следует относить общественно опасные, противоправные деяния, запрещенные Уголовным кодексом РФ и (или) Кодексом РФ об административных правонарушениях, которые оказывают или способствуют оказанию воздействия на принятие решения или совершение действия (бездействия) органом власти, органом местного

⁹⁶ Однако, как было отмечено ранее, диссертант не выделяет цель в качестве существенного признака терроризма.

⁹⁷ См.: Шевченко И.В. Уголовная ответственность за террористическую деятельность. М.: Юрлитинформ, 2011. С. 15-16.

самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом.

Кроме того, необходимо закрепить исчерпывающий перечень таких преступлений (правонарушений) террористической направленности в Федеральном законе РФ № 35-ФЗ, который следует приводить в соответствие с положениями УК РФ, КоАП РФ.

§2. Формы и виды терроризма

Ученые издавна пытались раскрыть сущность изучаемых явлений с помощью различных инструментов познания, одним из которых выступает классификация. Занимая очень важное место в познавательном процессе, она позволяет глубже осмыслить сущность изучаемого явления путем разделения его на виды, основой которого выступают различные признаки. Как одно из средств (инструментов) развития научного знания, классификация активно используется философскими, социальными, юридическими и другими науками.

Детальное изучение феномена терроризма невозможно без его классификации. В настоящее время авторами, изучающими терроризм как многоаспектное и негативное явление, разработано множество классификаций терроризма по различным основаниям. Однако некоторые исследователи отказываются от данного метода познания терроризма в связи со стремительным изменением сущности и форм его проявлений. Безусловно, терроризм прошлого века отличается от современного, хотя и имеет с ним общие признаки⁹⁸. Но, несмотря на это, без классификации как метода познания трудно или практически невозможно разработать эффективные меры противодействия всем формам и видам терроризма, поскольку специфика последних предопределяет данные меры.

Понятие «терроризм» выступает в качестве родового по отношению к понятиям многих других видов терроризма, выделяемых на основе различных критериев. Следует заметить, что любая классификация терроризма является условной, поскольку так или иначе его выделяемые виды и формы соотносятся друг с другом, где некоторые являются частью других.

⁹⁸ См.: Устинов В.В. Международный опыт борьбы с терроризмом: стандарты и практика. М.: Юрлитинформ, 2002. С. 43.

Выступающая в качестве научного метода, классификация должна иметь логическую основу (все явления должны быть взаимосвязаны, иметь особенности, позволяющие разграничивать их)⁹⁹.

Истоки проблемы разделения терроризма на виды (формы) и выбора оснований такого деления связаны в первую очередь с отсутствием единообразного понимания сущности и основных его признаков на международном и национальном уровне, что не позволяет выбирать те признаки терроризма, которые могут выступать основанием для его деления на виды. Кроме того, в первых редакциях УК РФ 1996 г. терроризм представлял собой преступное деяние, тогда как сейчас понятие терроризма является общеправовым, а УК РФ предусматривает ответственность за различные преступления террористической направленности (к последним в том числе относят террористический акт). Подобные изменения в российском законодательстве, безусловно, также отражались на классификации терроризма, вследствие чего предлагаемые авторами виды терроризма периода, когда последний признавался в качестве преступления, могут иметь теоретическое и историческое значение, но практическое значения для анализа его современных видов – нет.

Кроме того, как изменчивое и многоликое явление, терроризм постоянно «обрастает» новыми формами насильственных и иных противоправных действий, направленных на достижение присущих террористам целей. В связи с этим возникают новые классификационные основания деления терроризма на виды и формы.

Специфика классификации терроризма как социального явления связана не только с его исторической изменчивостью и динамичностью, но и с разнообразием его национальных форм (учеными подчеркивается отличие европейского терроризма от, например, ближневосточного), а также с

⁹⁹ См.: Байрамкулов А.М. Уголовная ответственность сотрудников органов внутренних дел за преступления, совершаемые при исполнении служебных обязанностей. М.: Юрлитинформ, 2015. С. 43.

различной политической и идеологической ориентацией его исследователей¹⁰⁰.

Так, существует классификация, в основе которой лежит метод осуществления террористического деяния. По данному признаку выделяется физический и психологический терроризм. Физический терроризм выражается в применении непосредственного воздействия на тело человека или группы людей. Сущность психологического терроризма, по мнению Е.В. Белой, выражается в достижении устрашающего эффекта путем разрушения материальных объектов, а также в применении морально-психологического насилия¹⁰¹. На этой же основе В.И. Замковой и М.З. Ильичков выделяют физический и духовный терроризм.¹⁰²

Однако психологическое воздействие является неотъемлемой чертой любого вида терроризма, даже физического. Совершение террористического акта путем взрывов или поджогов (физический терроризм) сопровождается паникой со стороны населения, которая также используется в качестве инструмента для наиболее быстрого и эффективного достижения соответствующих целей¹⁰³. Поэтому такое разделение терроризма является в большей степени условным, хотя использование исключительно психологических методов воздействия становится все более распространенным.

Очень часто исследования авторов по вопросу деления терроризма на виды сводятся к выделению последних без указания на конкретные классифицирующие основания¹⁰⁴. Такая тенденция не позволяет не только определить критерии, по которым следует различать виды терроризма, но

¹⁰⁰ См.: Соломин Д.А. Противодействие терроризму в информационной сфере: дис. ... канд. политич. наук. М., 2004. С. 18.

¹⁰¹ См.: Белая Е.В. Феномен терроризма в современном обществе: дис. ... канд. социол. наук. М., 2005. С. 27.

¹⁰² См.: Замковой В.И., Ильичков М.З. Терроризм – глобальная проблема современности. М.: Гардарика, 1996. С. 8-51.

¹⁰³ На сегодняшний день в качестве целей террористического акта, согласно ч. 1 ст. 205 УК РФ, выделяют дестабилизацию деятельности органов власти или международных организаций либо воздействие на принятие ими решений.

¹⁰⁴ См.: Миньковский Г.М., Ревин В.П. Характеристика терроризма и некоторые направления повышения эффективности борьбы с ним // Государство и право. 1997. № 8. С. 86.

также тормозит возможность прогнозирования появления новых его видов и форм.

Так, В.В. Лунеев выделяет следующие виды терроризма: терроризм по политическим мотивам, уголовный, националистический, «воздушный», международный, государственный и т.д.¹⁰⁵ Данный перечень не имеет в своей основе какого-либо единого критерия, где в качестве последнего выступают и мотив, и цель, и пространство действия, и т.п.

Итальянским ученым А. Кассизем была предложена классификация, в основе которой лежат мотивы и цели террористической деятельности¹⁰⁶. Им выделены следующие виды: терроризм, движущей силой которого является идеология; терроризм, имеющий целью достижение национальной независимости; терроризм «во имя самоопределения народов»; терроризм вооруженных групп и движений, борющихся против репрессивных режимов. Очевидная ошибка такого деления терроризма на виды выражается в том, что идеология является неотъемлемым признаком любого его вида или формы. Терроризм есть идейно-мотивированное движение, и выделение его одного вида, где движущей силой выступает идеология, в корне неверно. Верным было бы утверждение, что они различаются сущностной составляющей такой идеологии (это может быть религиозное составляющее, этническое или др.).

Прослеживается также тенденция смешения понятий «террор» и «терроризм» при выделении видов последнего. Так, Т.С. Бояр-Созонович выделяет следующие виды терроризма:

1) государственный, при котором террористическая деятельность осуществляется государством или при поддержке государства;

2) групповой (или организационный), к которому следует относить террористическую деятельность, осуществляемую группами или

¹⁰⁵ См.: Лунеев В.В. Терроризм и организованная преступность: национальный и транснациональный аспекты // Организованная преступность, терроризм и коррупция: криминологический ежеквартальный альманах. 2003. № 7 С. 3-19.

¹⁰⁶ См.: Cassese A. Terrorism, Politics and law: The Achille Lauro Affair. Cambridge: Polity Press, 1989. P. 143.

организациями частных лиц, не пользующихся поддержкой государства (так называемый оппозиционный терроризм);

3) стихийный (индивидуальный), осуществляемый частными лицами¹⁰⁷.

Основой такой классификации выступает, как видится, специфика субъекта террористической деятельности. В первом случае это субъект, пользующийся поддержкой государства, а в других – негосударственные субъекты. Негосударственные субъекты могут быть представлены в виде организаций или иных объединений, а также отдельных частных лиц (индивидуальное совершение террористических актов). Представляется, что в отношении государственных субъектов следует говорить о терроре, а не о терроризме¹⁰⁸.

Все предлагаемые авторами классификации терроризма имеют теоретическое и практическое значение. Из анализируемых классификаций следует различать общие, классификации на основании существенных признаков терроризма и классификации на основании второстепенных (но не менее значимых) признаков терроризма.

Самая общая и масштабная классификация терроризма связана с его разделением на международный и внутригосударственный. Внутригосударственный терроризм характеризуется деятельностью оппозиции против существующей политической системы. Кроме того, данный вид терроризма может быть представлен междоусобной деятельностью противоборствующих организаций, не находящихся у власти¹⁰⁹.

Международный характер терроризму придается в том случае, если:

1) преступление террористическое направленности совершается на территории иностранного государства;

¹⁰⁷ См.: Бояр-Созонович Т.С. Проблема классификации современного терроризма. М.: Университет дружбы народов им. Патриса Лумумбы, 1989. С. 11.

¹⁰⁸ См.: Назаркин М.В. Криминологическая характеристика и предупреждение терроризма: дис. ... канд. юрид. наук. М., 1998. С. 46.

¹⁰⁹ См.: Коссе В.О. Терроризм: социально-генетический и типологический анализ: дис. ... канд. философ. наук. Н. Новгород, 2004. С. 81.

2) преступление террористической направленности совершено в отношении лиц, пользующихся международной защитой¹¹⁰;

3) подготовка к преступлению террористической направленности (например, террористическому акту) ведется в одном государстве, а осуществляется в другом;

4) совершив преступление террористической направленности в одном государстве, террорист укрывается в другом и встает вопрос о его выдаче¹¹¹.

При характеристике международного терроризма исследователями также выделяют региональный, посягающий на безопасность нескольких государств, относящихся к одному географическому региону¹¹².

Как было отмечено ранее, терроризм есть идеологически обоснованная практика воздействия. Идеология, лежащая с основе терроризма, представляет собой систему взглядов и идей, оправдывающих или обосновывающих использование насилия и иных методов (инструментов) воздействия. Итак, по мотивам, составляющим идеологию терроризма, следует выделять:

- религиозный (в основе которого могут лежать убеждения о превосходстве одной религии над другой или о действительном или мнимом ущемлении прав и интересов какой-либо религиозной группы). Американский исследователь Дж. Пост предлагает выделять в этой группе терроризм фундаменталистских религиозных объединений (например, Аль-Каиды, группировки ХАМАС и «Хезболла»), а также объединений, исповедующих новые религии (например, Аум-Сенрике)¹¹³;

¹¹⁰ См.: Конвенция о предотвращении и наказании преступлений против лиц, пользующихся международной защитой, в том числе дипломатических агентов (принята резолюцией 3166 (XXVIII) Генеральной Ассамблеи ООН от 14 декабря 1973 года) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. XXXIII. М., 1979. С. 90-94 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

¹¹¹ См.: Моджорян Л.А. Указ. соч. С. 17.

¹¹² См.: Матчанова З.Ш. Факторы распространения терроризма в современной России: криминологический анализ: дис. ... канд. юрид. наук. СПб., 2015. С. 48.

¹¹³ См.: Post J. Differentiating the threat of chemical and biological terrorism: Motivations and constraints // Peace and Conflict: Journal of Peace Psychology. 2002 а. №8. P. 187-200.

- этнический или национальный (в основе которого могут лежать убеждения о превосходстве одного этноса или нации над другими или о действительном или мнимом ущемлении какой-либо этнической группы или нации). Как отмечает Ю.М. Антонян чаще всего такие террористы отстаивают свои личные интересы, а отнюдь не желания большинства из их народа, который может даже не знать о том, что ему нужна независимость¹¹⁴;

- политический (в основе которого могут лежать убеждения о действительном или мнимом несоответствии представителей власти (органов государственной власти, органов власти субъекта, политических деятелей и т.д.) общественным интересам). В этой связи выделяют ультраправый и ультралевый терроризм;

- идеалистический (в основе которого могут лежать убеждения о необходимости переустройства мира, достижения «справедливости»)¹¹⁵.

Помимо вышеназванных, в данную классификацию могут входить и иные виды терроризма, различающиеся по мотивам, составляющим их идеологию, например, корыстно-мотивированный терроризм.

Специальный объект воздействия также является сущностным, неотъемлемым признаком терроризма. По своей направленности следует различать терроризм, связанный с воздействием на принятие решения или совершения действия (бездействия): органом власти; органом местного самоуправления; международной организацией; социальной группой; юридическим лицом; физическим лицом.

Не исключено также воздействие одновременно на несколько из названных объектов¹¹⁶.

С.У. Дикаев в своей монографии приходит к заключению о том, что проблемы, связанные с неединообразными подходами к классификации

¹¹⁴ См.: Антонян Ю.М., Смирнов В.В. Терроризм сегодня. М.: ВНИИ МВД России, 2000. С. 27.

¹¹⁵ См.: Там же. С. 28.

¹¹⁶ См.: Комиссаров В.С. также приводит в своих исследованиях классификацию терроризма по объекту, выделяя преступления, где в качестве потерпевшего выступает специальный субъект, и преступления, по которым потерпевшие относятся к неопределенно широкому кругу лиц. См.: Комиссаров В.С. Терроризм, бандитизм, захват заложников. М.: Кросна-Лекс, 1997. С. 64.

терроризма, исходят также от смешения данного понятия с одним из его проявлений во внешнем мире – террористическим актом¹¹⁷. Безусловно, как негативное явление, терроризм проявляется в совершении преступлений террористической направленности, а также совершении иных противоправных деяний. Помимо видов терроризма, следует также говорить о его формах, характеризующихся специфичными средствами, методами, инструментами воздействия, пространством действия и др. Здесь следует говорить о второстепенных, но не менее значимых, признаках терроризма.

Как развивающаяся система, любая классификация является динамичной категорией, что связано с изменениями, которые происходят в самом подвергающемся классификации явлении, а также с получением новых знаний и информации о нем. Терроризм, выступающий составляющей частью предмета изучения данного диссертационного исследования, не является исключением. Вышеназванные критерии деления терроризма на формы (в зависимости от средств, методов, инструментов воздействия, пространства действия и т.п.) в большей степени подвергаются изменениям в связи с развитием и внедрением новых технологий, освоением новых видов оружия, всеобщим информационным оснащением и т.д.

По субъектному составу выделяют терроризм индивидуальный и коллективный. Последний, в свою очередь, подразделяется на групповой и организованный¹¹⁸.

По месту (пространству) осуществления (иначе – по среде протекания) террористической деятельности (в частности, преступлений террористической направленности) следует разделять терроризм на: воздушный, морской, наземный, информационный и др.¹¹⁹.

¹¹⁷ См.: Дикаев С.У. Террор, терроризм и преступления террористического характера (криминологическое и уголовно-правовое исследование). СПб.: изд-во Юридический центр Пресс, 2006. С. 59.

¹¹⁸ См.: Матчанова З.Ш. Указ. соч. С. 48.

¹¹⁹ См.: Попов И.В. География современного терроризма в странах европейского союза: дис. ... канд. географич. наук. М., 2009. С. 40; Требин М.П. Указ. соч. С. 30-36.

По средствам, применяемым при совершении террористических актов и иных преступлений террористической направленности, а также иных деяний, запрещенных законом или иными правовыми актами:

- с использованием обычных средств вооружения (огнестрельного оружия и др.);
- оружия массового поражения¹²⁰ (биологического, химического, ядерного оружия и др.);
- новейшего технологического оружия (например, военной техники, управляемой компьютером или иным техническим устройством; с использованием информационных технологий, информации и т.д.) и др.

На основе данной классификации исследователями выделяются следующие виды терроризма: химический, биологический, информационный, вооруженный (с использованием обычных средств вооружения – огнестрельного, холодного оружия, взрывчатых веществ и т.д.)¹²¹.

Исходя из вышеизложенного представляется возможным выделение информационного терроризма как формы терроризма на основании двух критериев: пространства осуществления и средств, применяемых террористами, террористическими организациями (сообществами).

На сегодняшний день информационный терроризм выделяется многими исследователями в качестве вида (или формы) терроризма. Однако в теории наблюдаются сложности с определением его сущности¹²², связанные в первую очередь с различными (иногда, противоположными) подходами к пониманию информационного пространства. Неединообразное понимание сущности и основных признаков информационного терроризма влечет за

¹²⁰ См.: Нардина О.В. Формирование общегосударственной антитеррористической системы. СПб.: изд-во Юридический центр Пресс, 2011. С. 37.

¹²¹ См.: Сорока Е.Ю. Особенности и тенденции эволюции современного терроризма: дис. ... канд. политич. наук. М., 2006. С. 57.

¹²² Роль превентивных мер противодействия информационному терроризму не адекватна степени угроз информационной безопасности, что связано с недостаточным изучением данного феномена. См.: Шамов М.И. Государственная стратегия и политические технологии предупреждения информационного терроризма в современном российском обществе: автореф. дис. ... канд. политич. наук. Н. Новгород, 2007. С. 7.

собой объективные трудности в разработке эффективных мер противодействия данному негативному явлению.

В связи с этим представляется необходимым более детально рассмотреть вопрос содержания понятия информационного пространства, а также средств (инструментов), применяемых террористами, террористическими организациями (сообществами) в информационном пространстве.

ГЛАВА 2. ПОНЯТИЕ, ПРИЗНАКИ И ВИДЫ ИНФОРМАЦИОННОГО ТЕРРОРИЗМА

§1. Понятие информационного терроризма: информационное пространство как платформа террористической деятельности

С начала XXI века российские исследователи в области террологии¹²³ стали акцентировать внимание на новой, не до конца на тот момент исследованной форме терроризма – информационном терроризме. В настоящее время информационный терроризм занял свою устойчивую позицию в классификации форм (а иногда – и видов) терроризма. Такие исследователи, как Д.А. Соломин, А.В. Федоров, С.И. Грачев, Е.А. Роговский, А.И. Маляров, Е.В. Белая и другие, выделяют информационный терроризм на основе различных классифицирующих оснований (чаще всего ими выступают средства воздействия)¹²⁴. Как отмечает А. Кота, информационный терроризм на сегодняшний день является одной из самых опасных форм терроризма, что обусловлено его «функционированием» в интеллектуальной сфере¹²⁵.

Между тем анализ научных работ вышеназванных и других авторов свидетельствует о неединообразном (порой – и абсолютно противоположном) понимании сущности и отличительных признаков информационного терроризма, что детерминировано его сложной природой.

¹²³ Террология есть наука о терроризме как особом социальном феномене (явлении), о его сущности, тенденциях, формах, целях, причинах. См.: Лекция по террологии [Электронный ресурс]. URL: <http://www.mylect.ru/polytolog/obchee/434-terrologiya.html> (дата обращения: 27.05.2016).

¹²⁴ См.: Соломин Д.А. Указ. соч. С. 32-33; Федоров А.В. Супертерроризм: новый вызов нового века. Научные записки пир-центра. М.: изд-во Права человека, 2002. С. 8; Грачев С.И. Терроризм и контртеррористическая деятельность: вопросы теории: учебное пособие. Н. Новгород: ФМО/ИСИ ННГУ им. Н.И. Лобачевского, 2010. С. 100, 112, 118; Роговский Е.А. Россия в борьбе с международным терроризмом: грани повышения позитивного образа страны // Электронный научный журнал «Россия и Америка в XXI веке». 2007. №3 [Электронный ресурс]. URL: <http://www.rusus.ru/?act=read&id=66> (дата обращения: 11.04.2016); Маляров А.И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации: автореф. дис. ... канд. юрид. наук. Краснодар, 2008. С. 4; Белая Е.В. Указ. соч. С. 29.

¹²⁵ См.: Цит. по: Глотина И.М. Информационный терроризм и его влияние на экономику // Проблемы современной экономики. 2014. № 3 (51). С. 133.

Представляется возможным систематизировать существующие на сегодняшний день исследования и выделить четыре точки зрения по заявленной проблеме.

Первая *характеризует информационный терроризм как кибертерроризм*¹²⁶. Данной точки зрения придерживаются такие авторы, как А.В. Федоров, Д.А. Соломин, С.И. Грачев, И.Н. Панарин, Л.Г. Панарина, Е.А. Роговский, С.Г. Туронок, Е.В. Старостина и др.¹²⁷

Уязвимость исследуемой позиции видится в поверхностном изучении отличительных признаков информационного терроризма, а равно – в неодинаковом понимании сущности, границ и признаков информационного пространства, выступающего особой платформой террористической деятельности.

Само по себе понятие пространства как сложной межотраслевой категории исходит из философии и физики, но с течением времени оно стало использоваться многими сферами и областями знаний, в том числе и правом. Затруднения при определении сущности понятия пространства, в частности – информационного, связаны с различными трактовками его содержания: техническими, экономическими, социальными, правовыми, политическими и др.

В праве понятие пространства, в первую очередь, раскрывается в связи с принципом действия правовых норм в пространстве. В данном случае его сущность характеризуется наличием границ и протяженностью, представляя

¹²⁶ Как отмечает М.Б. Касенова подобное понимание информационного терроризма сложилось в связи с спецификой перевода иностранных понятий с приставкой кибер- (*cyberspace, sybersecurity, cyberwar, cyberterrorism, etc.*) на русский язык. Например, вместо понятия киберпространства в Проекте Конвенции об обеспечении международной информационной безопасности (концепции), представленной Российской Федерацией в ООН 22 сентября 2011 г., используется понятие информационного пространства. См.: Касенова М.Б. Трансграничное управление интернетом: основные термины и понятия // Юридический мир, 2014. № 2 [Электронный ресурс]. URL: <http://www.center-bereg.ru/h31.html> (дата обращения: 18.06.2015).

¹²⁷ См.: Федоров А.В. Указ. соч. С. 8; Соломин Д.А. Указ. соч. С. 32; Грачев С.И. Указ. соч. С. 100; Панарин И.Н., Панарина Л.Г. Информационная война и мир. М.:ОЛМА-ПРЕСС, 2003. С. 317; Роговский Е.А. Указ соч. [Электронный ресурс]. URL: <http://www.rusus.ru/?act=read&id=66> (дата обращения: 11.04.2016); Туронок С.Г. Информационный терроризм: выработка стратегии противодействия // Общественные науки и современность. 2011. № 4. С. 132 [Электронный ресурс]. URL: <http://ecsocman.hse.ru/data/2014/01/16/1251303793/Turonok.pdf> (дата обращения: 11.04.2016); Старостина Е.В. Терроризм и кибертерроризм: угроза международной безопасности // Центр исследования компьютерной преступности [Электронный ресурс]. URL: <http://www.crime-research.ru/articles/starostina/3> (дата обращения: 11.04.2016).

тем самым определенную территорию. Названные признаки пространства позволяют решать крайне важные проблемы, связанные с юрисдикцией, регулированием и охраной общественных отношений на определенной территории. Разделение всех территорий в зависимости от правового режима на государственные, территории со смешанным и международным режимом позволяет определять границы действия тех или иных правовых норм в пространстве.

Понятие информационного пространства было известно человечеству еще до октября 1969 г., когда несколько ученых Калифорнийского и Стэнфордского университетов смогли отправить первое в истории существования ЭВМ сообщение, что послужило началу формирования сети Интернет¹²⁸. До этого знаменательного для истории человечества события информационное пространство связывали с такими средствами обращения информации, как печатные газеты, журналы, иные средства коммуникации (например, листовки, объявления и др.). Возникновение же сети Интернет (и других локальных сетей) способствовало более быстрому, неконтролируемому обращению информации не только в пределах одной страны, но и всего мира. В связи с этим стало важным установить сущность и основные признаки информационного пространства для эффективного регулирования и охраны общественных отношений в данной сфере.

В настоящее время действует более 10 конвенций о защите от терроризма на земле, в воздухе и на море¹²⁹. Вопросы, связанные с определением сущности воздушного пространства, разрешены в том числе на национальном уровне, о чем свидетельствуют положения ст. 15 Воздушного Кодекса Российской Федерации. Вопросы содержания понятия морского пространства регламентированы положениями международного права. Вопросы содержания понятия наземного пространства в большей степени

¹²⁸ См.: Иванов А.К. Глобальное информационное пространство и его место в современном международном праве // Ползуновский вестник. Барнаул, 2005. № 1. С. 220.

¹²⁹ См.: Сочнев Д.В. Основные виды и наиболее распространенные формы международного терроризма // Полицейская и следственная деятельность. 2013. № 2 [Электронный ресурс]. URL: http://e-notabene.ru/pm/article_801.html (дата обращения 02.10.2015).

являются теоретическими, а в праве и законодательстве его содержание лишь подразумевается. Нормы о предотвращении, в частности, террористических актов в воздушном, морском и наземном пространстве закреплены в Федеральном законе № 35-ФЗ «О противодействии терроризму».

При этом уже не новой, но до конца не изученной остается сущность информационного пространства, понятие которого не разъяснено в действующем законодательстве. Между тем значение развития и защиты информационного пространства подчеркивается Доктриной информационной безопасности Российской Федерации, Проектом конвенции об обеспечении международной информационной безопасности (представленной Российской Федерацией), Правилами поведения в области обеспечения международной информационной безопасности и другими документами¹³⁰. Существующий подход не позволяет определить содержание таких имеющих международное значение понятий, как информационная война и информационный терроризм.

В некоторых источниках, в том числе экономических и информационных словарях, отмечаются затруднения в установлении сущности дефиниции «информационное пространство». На сегодняшний день данное понятие характеризуется высокой распространенностью и пониманием на уровне интуиции¹³¹. Между тем исследуемые в доктрине понятия информационного пространства отражают специфику той сферы научного знания, в рамках которой оно разрабатывалось (социологии, экономики, техники и т.п.). При этом законодательная база, связанная с терминологией в информационной сфере в Российской Федерации и на международном уровне, проработана слабо. Представленные выше

¹³⁰ Доктрина информационной безопасности Российской Федерации, утв. Президентом РФ В. Путиным 9 сентября 2000 г. № Пр-1895 // Рос. газета. 2000. 28 сент.; Проект конвенции об обеспечении международной информационной безопасности (концепция) [Электронный ресурс]. URL: <http://www.scrf.gov.ru/documents/6/112.html> (дата обращения: 02.10.2015); Правила поведения в области обеспечения международной информационной безопасности [Электронный ресурс]. URL: http://archive.mid.ru/brp_4.nsf/newsline/BA8A7E45ED6164CA43257DDC0050C89E (дата обращения: 02.10.2015).

¹³¹ См.: Ковалевский В.П., Буреш О.В., Жук М.А., Калиева О.М. Аккумуляция знаний в информационном пространстве предприятий региона. М.: Финансы и статистика, 2011. С. 27.

международные документы содержат размытую, несущественную информацию об угрозах безопасности информационного пространства. Однако последний предложенный Российской Федерацией Проект конвенции об обеспечении международной информационной безопасности несколько улучшил ситуацию. Несмотря на то что в терминах и определениях (статья 1) Проекта конвенции отсутствует понятие информационного пространства, был установлен очень подробный перечень возможных угроз международному миру и безопасности в этой сфере, из чего возникает возможность определить, что оно из себя представляет.

К основным информационными угрозами (статья 4) Проект конвенции относит:

- 1) противоправное использование информационных технологий;
- 2) противоправное воздействие в информационном пространстве на критически важные структуры государства;
- 3) психологическую обработку населения, дестабилизирующую общество;
- 4) использование информационного пространства в террористических, экстремистских и иных преступных целях;
- 5) распространение информации, разжигающей межнациональную, межрасовую и межконфессиональную вражду, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества;
- 6) приобретение контроля над национальными информационными ресурсами другого государства.

Таким образом, Проектом конвенции очерчивается некое смысловое поле данного понятия, определяя посредством перечисления возможных угроз некоторые признаки информационного пространства. Во-первых, оно характеризуется безграничностью, в чем выражается, собственно, специфика данного вида пространства. Сам характер предложенных данным проектом угроз определяет информационное пространство как уникальную по своей

природе сферы существования общественных отношений. Кроме того, информационное пространство характеризуется использованием информации, информационных технологий и (или) информационных ресурсов¹³². На доктринальном уровне исследователями также подчеркивается, что основным существенным компонентом информационного пространства выступают информационные ресурсы¹³³.

Таким образом, *информационное пространство* следует определять как *характеризующуюся безграничностью сферу существования общественных отношений, связанную с использованием информации, информационных технологий и информационных ресурсов*.

Сложившееся в доктрине понимание информационного терроризма как кибертерроризма обусловлено не только спецификой перевода иностранных слов на русский язык (как отмечает М.Б. Касенова), но и проблемами соотношения понятий информационного и кибернетического пространства.

Как и в отношении понятия информационного пространства вопрос содержания понятия киберпространства (или виртуального пространства) является непростым, поскольку отсутствует его единообразное понимание. Существующие на сегодняшний день международные документы, регламентирующие вопросы обеспечения кибербезопасности, не раскрывают понятия киберпространства. Несмотря на это, большинство авторов отмечают, что отличительным признаком исследуемого понятия выступает его связь с сетью Интернет (либо иной локальной или территориальной сетью), доступ к которым обеспечивается с помощью различных технических

¹³² В Концепции формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов закреплено понятие единого информационного пространства и определены составляющие его компоненты, которыми являются информационные ресурсы, информационные технологии и технические устройства, обеспечивающие доступ граждан и организаций к информационному пространству. См.: Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (одобрена решением Президента РФ от 23.11.1995 № Пр-1694). М., НТЦ «Информрегистр». 1996 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

¹³³ См.: Каткова М.В. Понятие «Информационное пространство» в современной социальной философии // Известия Саратовского университета. 2008. № 2. Т.8. С. 25; Джакупов Ж.А. Формирование и развитие единого информационного пространства юридического сообщества Российской Федерации (на примере ассоциации юристов России): автореф. дис. ... канд. юрид. наук. М., 2011. С. 7.

устройств¹³⁴. Кроме того понятие «киберпространство» связывают с понятием цифровых информационных ресурсов¹³⁵. На сегодняшний день Европейской Конвенцией по киберпреступлениям возможные угрозы в киберпространстве определены следующим образом: это правонарушения, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей данных, а также неправомерное использование указанных систем, сетей и данных, а также иные преступления и правонарушения, совершаемые с помощью или посредством компьютеров, компьютерных сетей, к которым относят мошенничество, плагиат, распространение детской порнографии и др.¹³⁶ Таким образом, конвенцией сфера киберпространства ограничена также исключительно сетью Интернет (или иной локальной или территориальной сетью связи компьютерных и иных технических устройств)¹³⁷. В науке правовое понятие киберпространства определяется как совокупность общественных отношений, возникающих в процессе использования и функционирования электронной компьютерной сети по поводу обращения информации¹³⁸.

Киберпространство как специфичная сфера существования общественных отношений характеризуется исходя из вышеизложенного следующими признаками:

¹³⁴ См.: Телешина Н.Н. Виртуальное пространство как объект контрольной деятельности государства: автореф. дис. ... канд. юрид. наук. Муром, 2011. С. 9.

¹³⁵ Цифровые информационные ресурсы – это переведенная в цифровой код информация в форме данных, баз данных и программно-информационных продуктов, которая обрабатывается с использованием средств вычислительной техники [Электронный ресурс]. URL: http://normative_reference_dictionary.academic.ru/87332/цифровые_информационные_ресурсы (дата обращения: 15.06.2016).

¹³⁶ Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве). Будапешт, 23 ноября 2001 года [Электронный ресурс]. URL: <http://mvd.gov.by/main.aspx?guid=4603> (дата обращения: 17.10.2015).

¹³⁷ Ошибочно связывать киберпространство исключительно с сетью Интернет. Как отмечалось исследователями еще в начале 21 века помимо сети Интернет существуют и иные электронные сети. См.: Савостицкий Ю.А. История развития глобальных компьютерных сетей // Информационное общество. 2000. № 4. С. 59.

¹³⁸ См.: Грибанов Д.В. Правовое регулирование кибернетического пространства как совокупности информационных отношений: дис. ... канд. юрид. наук. Екатеринбург, 2003. С. 125; Видами компьютерной сети выступают различные локальные и иные территориальные сети, объединяющие группы компьютеров. См.: Что такое компьютерная сеть [Электронный ресурс]. URL: <http://ict.edu.ru/ft/005119//ch1.pdf> (дата обращения: 19.04.2016).

1) связано с использованием информационных технологий, компьютерной информации, цифровых информационных ресурсов¹³⁹;

2) доступ к нему обеспечивается с помощью различных технических устройств, объединенных сетью Интернет (или иной информационно-телекоммуникационной сетью);

Киберпространство следует определять как *сферу существования общественных отношений, доступ к которой обеспечивается с помощью различных технических устройств, объединенных сетью Интернет или иной локальной или территориальной сетью, связанной с использованием информационных технологий, компьютерной информации и) цифровых информационных ресурсов*. Соотношение информационного пространства и киберпространства более подробно изложено в таблице (прил. 1; С. 239).

Таким образом, соотношение киберпространства и информационного пространства следует определять как часть и целое. Киберпространство выступает составным элементом, новейшей сферой существования общественных отношений, связанной с использованием исключительно компьютерной информации, цифровых информационных ресурсов и (или) информационных технологий. Из этого следует, что кибертерроризм выступает частью терроризма информационного.

Еще одна точка зрения определяет *понятие информационного терроризма как психологического* (А.Н. Кулибаба, О.Н. Алексеев, Д.В. Ольшанский, И.М. Глотина, М.И. Шапов и др.¹⁴⁰).

Следует заметить, что понимание информационного терроризма как исключительно психологического воздействия на население с помощью

¹³⁹ Именно такую дефиницию информации использует законодатель при характеристике преступлений, содержащихся в главе 28 УК РФ. Само по себе понятие «компьютерная информация» вызывает множество споров. Некоторые исследователи полагают целесообразным говорить об информации, обращающейся в Сети. См.: Рассолов И.М. Право и интернет: теоретические проблемы. М.: Норма, 2009. 383 с. [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

¹⁴⁰ См.: Кулибаба А.Н. Информационный терроризм [Электронный ресурс]. URL: <http://law.edu.ru/doc/document.asp?docID=1252544> (дата обращения: 11.04.2016); Алексеев О.Н. Международный терроризм и борьба с ним крупнейших государств тихоокеанского региона: дис. ... канд. политич. наук. Владивосток, 2013. С. 64; Ольшанский Д.В. Психология терроризма. СПб.: Питер, 2002. 288 с. [Электронный ресурс]. URL: http://scienceport.ru/files/psi_terror.pdf (дата обращения: 11.04.2016); Глотина И.М. Указ. соч. С. 134.

информации весьма спорно. Несмотря на то что исследователями уже не раз отмечалась сравнительно большая опасность именно психологического воздействия, террористическая деятельность в информационном пространстве не может и не должна ограничиваться исключительно распространением информации о насилии или искажением объективной информации¹⁴¹. В то же время, воздействие в виде пропаганды, вербовки, применения психологического насилия является неотъемлемой частью террористической деятельности в информационном пространстве¹⁴².

На уровне доктрины также существует мнение, согласно которому *информационный терроризм – это феномен информационного общества, это «лицо» современного терроризма, характеризующегося усовершенствованными средствами и способами совершения преступлений*¹⁴³. То есть информационный терроризм – это не форма (вид) терроризма, а качественная характеристика последнего. В связи с интеграцией большинства стран мира в международный информационный обмен все (как положительные, так и негативные) явления общественной жизни подверглись изменениям, связанным с усовершенствованиями, которые произошли в сфере информационных технологий. Иными словами, терроризм любого вида и формы всегда носит информационный характер¹⁴⁴. Нет сомнений в том, что терроризм есть своеобразная, крайне опасная форма манипуляции. Однако свидетельствовать о том, что террористическое воздействие всегда намеренно осуществляется при непосредственном участии СМИ и иной телекоммуникации, не представляется возможным. В этой связи можно привести следующую аналогию. Информационная война на протяжении всей истории человечества сопровождала вооруженные

¹⁴¹ Противоположного мнения придерживается М.И. Шамов. См.: Шамов М.И. Государственная стратегия и политические технологии предупреждения информационного терроризма в современном обществе: дис. ... канд. юрид. наук. Н. Новгород, 2007. С. 11-12.; Чубик А.П. Терроризм в информационном пространстве // Известия Томского политехнического университета. 2013. № 6. Т. 323. С. 119.

¹⁴² См.: Россошанский А.В. Риски и угрозы информационного терроризма // Человек. Сообщество. Управление. 2011. № 3. С. 101.

¹⁴³ См.: Воронина Т.П. Современный терроризм как феномен информационного общества // Материалы II Всероссийской научно-практической конференции. М.: Университетская книга, 2010. Т. I. С. 446-447.

¹⁴⁴ См.: Чубик А.П. Указ. соч. С. 119.

конфликты¹⁴⁵. Однако ее масштабы и последствия были значительно меньше, нежели в эпоху информационных технологий¹⁴⁶. Как отмечает И.Н. Панарин, информационная война выступает одним из средств мировой политики, направленной на достижение духовного, политического, финансового и экономического господства¹⁴⁷. Сегодня информационное противоборство государств достигло очень высокого уровня, сопровождая открытые вооруженные столкновения (например, грузино-осетинский конфликт, войну в Персидском заливе 1991 г.¹⁴⁸) и периоды так называемой «холодной войны»¹⁴⁹. Это же свойственно и современному терроризму. Информационное воздействие используется сложноструктурированными террористическими организациями и отдельно, и в качестве сопровождения классической террористической деятельности (совершения террористических актов путем взрывов или поджогов, захвата заложников и т.п.).

На сегодняшний день информационный терроризм получил значительный арсенал различных средств (инструментов) воздействия, из-за чего представляется необходимым рассматривать его как отдельную форму терроризма, нуждающуюся в детальном изучении и разработке эффективных мер противодействия.

Последняя точка зрения, суть которой сводится к тому, что *кибертерроризм и психологический терроризм являются видами информационного терроризма*, представляется, на наш взгляд, наиболее

¹⁴⁵ В рамках данного диссертационного исследования предлагаем придерживаться следующему определению информационной войны – противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам, ресурсам, критически важным структурам, подрыва политической, экономической и социальной систем, а также массовой психологической обработки населения с целью дестабилизации общества и государства (из Доклада Генерального секретаря ООН: А/55/140/Генеральная Ассамблея ООН: Пятьдесят пятая сессия. 2000. 10 июля). Цит. по: Бедрицкий А.В. Международные договоренности по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. № 4. С. 120.

¹⁴⁶ См.: Дементьева К.В. Информационная война // Журналистский ежегодник. 2014. № 3. С. 14.

¹⁴⁷ См.: Панарин И.Н. СМИ, пропаганда и информационные войны. М., 2012 [Электронный ресурс]. URL: http://propagandahistory.ru/books/Igor-Panarin_SMI--propaganda-i-informacionnye-voyny/ (дата обращения: 24.04.2016).

¹⁴⁸ См.: Лабуш Н.С. Информационная война как порождение нового времени и современных массмедиа технологий. Ч. 1. Продолжение политики средствами информационного насилия // Медиаскоп. 2015. № 2 [Электронный ресурс] URL: <http://mediascope.ru/?q=node/1739> (дата обращения: 05.07.2016).

¹⁴⁹ См.: Манойло А.В. Информационно-психологическая война в вооруженном конфликте в Южной Осетии // Власть. 2009. № 9. С. 83; Соловьев А.В. Информационная война: понятие, содержание, перспектива // Пространство и время. 2010. № 2. С. 77-78.

предпочтительной. Такое широкое понимание информационного терроризма позволяет охватить весь возможный спектр террористической деятельности в информационном пространстве¹⁵⁰. Данной точки зрения придерживаются следующие авторы: Е.В. Белая, А.И. Маляров, В. Цыганов, А.И. Примакин, В.Е. Кадулин, Ю.И. Жуков, В.И. Антюхов, Е.Л. Логинов и др.¹⁵¹.

На сегодняшний день к наиболее опасным угрозам международному миру и безопасности в информационном пространстве следует относить информационный терроризм и информационную войну. Первая, являющаяся предметом изучения данного диссертационного исследования, характеризуется противоправной деятельностью негосударственных субъектов в информационном пространстве. Такая деятельность должна являться террористической, то есть обладать всеми признаками, присущими терроризму.

Помимо этого, информационному терроризму присущи и иные отличительные признаки:

1) платформой информационного терроризма выступает информационное пространство, содержание которого было представлено выше;

2) воздействие как сущностный признак в том числе информационного терроризма, обладает определенной спецификой: инструментами (средствами) воздействия выступает информация, информационные ресурсы и информационные технологии.

Поскольку воздействие, осуществляемое в пределах информационного пространства, так или иначе содержит информационный элемент, следует говорить об информационном воздействии. Последнее в контексте

¹⁵⁰ Проектом конвенции об обеспечении международной информационной безопасности (ст. 9) определены возможные террористические угрозы, к которым отнесены: создание и функционирование интернет-ресурсов террористического характера, совершение компьютерных атак, а также иные угрозы использования информационного пространства в террористических целях.

¹⁵¹ См.: Белая Е.В. Указ. соч. С. 8; Маляров А.И. Указ. соч. С. 4; Цыганов В. Медиа-терроризм: терроризм и средства массовой информации. Киев: Ника-центр, 2004. С. 24-25; Примакин А.И., Кадулин В.Е., Жуков Ю.И., Антюхов В.И. Информационный терроризм: прошлое, настоящее, будущее // Вестник Санкт-Петербургского университета МВД России. 2000. № 1. С. 57-58; Логинов Е.Л. Проблемы противодействия информационному терроризму // Национальные интересы: приоритеты и безопасность. 2008. № 4. С. 75.

понимания сущности информационного терроризма характеризуется специальными средствами воздействия.

Информационный терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах информационного пространства, связанного с использованием информации, информационных технологий и (или) информационных ресурсов.

В целях оценки возрастающей угрозы информационного терроризма следует остановиться также на признаках, характеризующих общественную опасность исследуемого явления:

1. *Глобальная информатизация и прогресс в сфере развития информационных технологий.* Данный аспект всестороннего повсеместного проникновения информации и информационных технологий во все сферы жизни общества отмечается исследователями проблем обеспечения информационной безопасности уже довольно давно. Участие в формировании глобального информационного пространства принимают все государства, где существует понятие СМИ, информации и хотя бы один компьютер (или иное техническое устройство) с доступом в сеть Интернет. Между тем ученые все чаще акцентируют внимание на угрозах, которые возникают в связи с возрастающим прогрессом в сфере развития информационных технологий¹⁵². К таковым следует относить информационную войну, информационный терроризм и информационные преступления¹⁵³.

2. *Безграничность информационного пространства.* Информационное пространство не имеет привычных границ и территорий. С помощью

¹⁵² См.: Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 45.

¹⁵³ См.: Кубышкин А.В. Международно-правовые проблемы обеспечения информационной безопасности государств: дис. ... канд. юрид. наук. М., 2002. С. 10.

различных технических устройств, обеспечивающих доступ в сеть Интернет, находящихся на территории, например, России, можно проникнуть в информационную систему Великобритании, посетить в том числе правительственные сайты, сайты различных организаций и т.п. Кроме того, средства массовой информации спроецировали свою деятельность, в том числе и на сеть Интернет. Независимость от национальных границ является очень привлекательной для преступников; свободный обмен информации в пространстве выступает в качестве движущей силы прогресса. Знание есть сила, и знание не что иное, как информация.

Пространство, формирующееся в связи с возрастающим процессом информатизации, лишено его привычных геополитических признаков, таких как территориальные границы. Оно символично. Однако существуют запреты, основанные на нормах международного и национального права, не позволяющие вторгаться в чужое информационное пространство (охрана частной жизни), а также получать доступ к информации, составляющей сведения, содержащие какую-либо тайну (государственную, адвокатскую, банковскую и т.п.). Проблема возникает в связи со слабостью законодательного обеспечения защиты информации от подобных вторжений, а также в связи с неодинаковым отношением различных стран к процессу глобальной информатизации.

3. *Различный уровень информатизации, который прямо пропорционален уровню законодательного обеспечения защиты информации от её неправомерного использования или воздействия на неё.* Как известно, все страны мира различаются по уровню социально-экономического развития на развитые страны с рыночной экономикой, страны с переходной экономикой и развивающиеся страны. Примерно такая же градация стран происходит в связи с присущим им уровнем информатизации и развитием информационных технологий. В странах, характеризующихся сильным процессом информатизации, действуют национальные стратегии обеспечения информационной безопасности, постоянно совершенствуется

законодательство в сфере ее обеспечения. В то же время, существуют страны, где процесс информатизации очень слабый, соответственно информационное законодательство либо вообще отсутствует, либо находится в «зачаточном» состоянии.

По данным одного российского сайта число пользователей сети Интернет в России от 18 лет и старше составляет 70% от всего населения страны¹⁵⁴. Например, в Нигерии, являющейся страной, где законодательство об обеспечении информационной безопасности отсутствует, по некоторым данным число населения, имеющего доступ к сети Интернет, составляло 30-40% в 2013 году¹⁵⁵ (население Нигерии в тот момент составляло 172 млн человек). Различие в законодательном обеспечении информационной безопасности в условиях информационного пространства, где, как было ранее отмечено, привычные территориальные границы отсутствуют, способствует возникновению «инкубатора» для опытных киберпреступников. Исследователями уже отмечался факт активного использования представителями и участниками террористических организаций (например, Аль-Каиды) неконтролируемого со стороны правительства доступа в Интернет в целях финансирования, сообщения, вербовки и совершения преступлений¹⁵⁶. Отсутствие либо недостаточное законодательное обеспечение информационной безопасности отдельных стран, которые так или иначе являются участниками формирования глобального информационного пространства, могут привести к безнаказанности лиц, которые уже используют ослабленную информационную платформу для совершения преступлений.

4. Доступность вычислительных и иных устройств, необходимых для проникновения в информационные системы, а также иных средств

¹⁵⁴ См.: Количество пользователей интернет России. Обновление от 15.04.2016 года [Электронный ресурс]. URL: http://www.bizhit.ru/index/users_count/0-151 (дата обращения 05.07.2016).

¹⁵⁵ См.: Chijioko Oluoch. Internet access set to triple in Nigeria [Электронный ресурс]. URL: <http://af.reuters.com/article/topNews/idAFJJOE75E0H920110615> (дата обращения: 27.05.2016).

¹⁵⁶ См.: Carr J. Inside cyberwarfare. Sebastopol: O'Really, 2012. P. 255-256.

коммуникации. Относительная дешевизна ресурсов доступа и простота в использовании. Безусловным достоинством сети Интернет (представляющей собой всемирную компьютерную сеть, объединяющую тысячи сетей всего мира) является быстрота передачи и получения, удобство хранения информации, а также дешевизна ресурсов доступа к ней. Помимо этого, в большинстве стран мира «выход» в сеть Интернет анонимный и свободный (например, при подключении к WiFi не нужно вводить какие-либо личные данные или получать разрешение у провайдера), с помощью нее можно привлечь внимание большей аудитории. Слабый уровень цензуры в сети Интернет за распространяемой информацией активно используется преступниками.

Не оставляя без внимания факта широкого понимания информационного пространства, не ограничивающегося сетью Интернет и компьютерной сетью, отметим и возможность использования преступниками иных средств коммуникации: печатных изданий СМИ, радио, телевидения, книг, листовок, информационных ресурсов (например, для пропаганды насилия, возбуждения ненависти или вражды к определенной социальной группе, обмена информации).

Все названные признаки свидетельствуют о возрастающей угрозе безопасности информационного пространства и необходимости принятия мер по формированию, во-первых, теоретической базы (понятийно-категориального аппарата), а во-вторых, специализированных (в том числе уголовно-правовых) мер противодействия информационному терроризму, информационной войне и информационным преступлениям.

Помимо пространственного критерия, основой выделения информационного терроризма могут выступать характерные только для него инструменты воздействия, применяемые при совершении, в частности, террористических актов и иных преступлений (правонарушений) террористической направленности.

В первую очередь таким средством («орудием») может выступать информация. Собственно, информация является исходным понятием (наравне с понятием терроризма) по отношению к понятию информационного терроризма.

В настоящее время в УК РФ информация и иные формы ее выражения (сведения, сообщения, данные) могут быть предметом некоторых преступных деяний, относящихся к преступлениям против конституционных прав и свобод человека и гражданина; преступлений в сфере экономической деятельности; преступлений против основ конституционного строя и безопасности государства; преступлений в сфере компьютерной информации и др. Кроме того, иные отрасли права (гражданского и административного) активно используют понятие информации. В первую очередь это связано со стремительным развитием и с внедрением информационных технологий во все сферы жизни общества. Однако проведенный анализ использования понятия «информация» в правовой регламентации каких-либо явлений свидетельствует о неодинаковом определении его сущности. Для уголовного законодательства наличие двусмысленности, неопределенности содержания терминов при описании конкретных составов преступлений является недопустимым, в связи с чем понятие информации, а также наравне с ним и такие понятия, как «информационные технологии», «информационные ресурсы» требуют более детального рассмотрения в рамках данного диссертационного исследования.

§2. Средства (инструменты) информационного воздействия

Воздействие в уголовном праве рассматривается в двух направлениях: позитивном и негативном. Первое отождествляется с институтом уголовно-правового воздействия¹⁵⁷, второе – с преступным (криминальным) воздействием¹⁵⁸. В рамках данного диссертационного исследования представляется необходимым рассмотреть второе направление исследуемого понятия.

О криминальном воздействии в УК РФ упоминается при характеристике таких составов преступлений, как террористический акт (ст. 205) и уничтожение или повреждение лесных насаждений (ст. 261). Кроме того, в доктрине сущностное содержание понятий уголовно-правового принуждения¹⁵⁹, понуждения¹⁶⁰, психического и физического насилия¹⁶¹ раскрывается через более широкое понятие «воздействия».

В Толковом словаре русского языка понятие «воздействовать» раскрывается как «оказав влияние, добиваться необходимого результата»¹⁶². Таким образом, понятия воздействие и влияние (а равно, как отмечают

¹⁵⁷ Всестороннему исследованию институт уголовно-правового воздействия подвергался со стороны таких ученых, как: Н.А. Лопашенко, М.В. Бавсун, В.К. Дуюнов, С.В. Векленко, Б.Т. Разгильдиева и др. См.: Лопашенко Н.А. Основы уголовно-правового воздействия: уголовное право, уголовный закон, уголовно-правовая политика. СПб.: Юридический центр Пресс, 2004. С. 166; Бавсун М.В. Понятие и содержание уголовно-правового воздействия на преступность // Вестник Томского государственного университета. 2010. № 336. С. 102; Дуюнов В.К. Уголовно-правовое воздействие: теория и практика. М.: Научная книга, 2003. С. 28; Векленко С.В. О повышении эффективности уголовно-правового воздействия // Противодействие преступности: уголовно-правовые, криминологические и уголовно-исполнительные аспекты: Материалы III Рос. конгр. уголовного права. М., 2008. С. 234; Разгильдиев Б.Т. Уголовно-правовое воздействие и его пределы // Известия вузов. Правоведение. 2011. № 2. С. 175.

¹⁵⁸ Частные вопросы криминального воздействия исследовались в работах таких авторов, как А.Ю. Федоров, А.В. Макиенко, Н.А. Лопашенко, М.В. Кроз, Н.А. Ратинова, О.Р. Онищенко, Л.В. Сердюк и др. См.: Федоров А.Ю. Криминальное манипулирование в сфере экономической деятельности: криминологическая характеристика и предупреждение: автореф. дис. ... канд. юрид. наук. Омск, 2006. С. 6; Макиенко А.В. Уголовно-правовые и криминологические проблемы предупреждения криминального информационного воздействия преступных сообществ: дис. ... канд. юрид. наук. М., 1997. С. 13; Лопашенко Н.А. Разграничение лжепредпринимательства и мошенничества // Законность. 1997. № 9. С. 18; Кроз М.В., Ратинова Н.А., Онищенко О.Р. Криминальное психологическое воздействие. М.: Юрлитинформ, 2008. С. 36; Сердюк Л.В. Указ. соч. С. 23.

¹⁵⁹ См.: Попов Д.В. К вопросу о соотношении уголовно-правовых понятий: принуждение и насилие // Актуальные вопросы уголовного процесса современной России. Уфа, 2003. С. 51; Кругликов Л.Л. Преступления против личности. Ярославль: ЯрГУ, 1998. С. 67.

¹⁶⁰ См.: Радостева Ю.В. Указ. соч. С. 11.

¹⁶¹ См.: Пионтковский А.А., Меньшагин В.Д. Указ. соч. С. 722; Радостева Ю.В. Указ. соч. С. 82.

¹⁶² См.: Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. М.: Азбуковник, 1999. С. 92.

некоторые исследователи, и понятие действия) используются как синонимы¹⁶³. Однако, будучи таковыми на уровне обыденного общественного сознания, они являются синонимичными лишь в определенной части. Так, понятия действия и влияния являются более широкими по содержанию, нежели понятие воздействие. Последнее всегда носит деятельный характер¹⁶⁴. Причем, по справедливому замечанию А.Н. Леонтьева, такая деятельность всегда предметна, то есть связана с оказанием влияния на тот или иной объект для достижения поставленной цели¹⁶⁵.

По своему существу воздействие не несет в себе исключительно негативного содержания, являясь частью процесса взаимодействия людей. Положительная направленность воздействия проявляется, например, в педагогических, воспитательных процессах, в связи с чем уместно разделять воздействие на преступное и не преступное. Исходя из содержания доктринальных исследований следует выделять физическое и психическое (или психологическое)¹⁶⁶ преступное воздействие¹⁶⁷.

Само по себе воздействие как процесс оказания влияния может быть рассмотрен с различных позиций. В рамках данного диссертационного исследования нас интересует такое воздействие, которое составляет сущность терроризма. Как было отмечено ранее, специфика воздействия в терроризме проявляется в его опосредованном характере, что обусловлено двойственностью объекта (тактическом и стратегическом) такого воздействия, а также его идеологической обоснованностью.

¹⁶³ См.: Бобраков И.А. Воздействие преступников на свидетелей и потерпевших и криминалистические методы его преодоления: дис. ... канд. юрид. наук. М., 1997. С. 10.

¹⁶⁴ См.: Там же. С. 11.

¹⁶⁵ См.: Леонтьев А.Н. Деятельность. Сознание. Личность. М.: Политиздат, 1975. С. 157.

¹⁶⁶ Как правило, понятия психологического и психического воздействия в научных словарях используются как синонимы. Однако, преимущественно о психологическом воздействии говорится в специализированной психологической литературе. См.: Кроз М.В., Ратинова Н.А, Онищенко О.Р. Указ. соч. С. 36.

¹⁶⁷ При характеристике таких уголовно-правовых понятий как принуждение и насилие, авторы подразделяют их на физическое и психическое, в основе чего лежит объект воздействия. См.: Радостева Ю.В. Указ. соч. С. 11.

Информационному воздействию присущи и иные отличительные черты, определяемые особыми средствами (инструментами) такого воздействия. В первую очередь, таким средством (инструментом) воздействия выступает информация. На сегодняшний день информация и знания являются основным предметом человеческого труда¹⁶⁸. Содержание правовых норм, в том числе и уголовных, претерпевает значительные изменения в условиях усложняющейся информационно-электронной реальности¹⁶⁹. Однако по мнению некоторых исследователей, процесс нормотворчества в сфере обеспечения информационной безопасности должен продолжаться, поскольку информация как сложноорганизованная система регулируется различными отраслями права¹⁷⁰.

Слово «информация» происходит от латинского *informare*, что означает «придавать вид, форму, обучать, мыслить, воображать»¹⁷¹. Впервые научное изучение понятия информации было осуществлено гуманитариями. В начале XX в. под информацией в журналистике понималось «описание фактов» или «новости»¹⁷². Уже тогда стали формироваться признаки информации, которые позднее использовались иными сферами знаний (математикой, кибернетикой, правом).

Прежде всего было установлено, что информация должна обладать признаком *новизны*, под чем подразумевались «...неожиданные, принципиально не похожие на уже известные» факты. Общим для понятия новизны явилось новое понятие «*информационная ценность*», которое ввел в 1928 году А. Курс. Под ним он понимал «...неповторимое качество явления, выделяющее его из повторяющегося ряда»¹⁷³. Таким образом, новизна и

¹⁶⁸ См.: Букалерева Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. ... д-ра юрид. наук. М., 2007. С. 64.

¹⁶⁹ См.: Степанов О.А. Ключевые аспекты правового регулирования использования и развития информационно-электронных технологий // Государство и право. 2004. № 4. С. 70.

¹⁷⁰ См.: Букалерева Л.А. Указ. соч. С. 72.

¹⁷¹ См.: Полонников Р.И. Феномен информации и информационного взаимодействия (введение в семантическую теорию информации). СПб.: Анатолия, 2001. С. 6.

¹⁷² См.: Гарри А. Н. Что такое информация // Журналист. 1928. № 1. С. 42.

¹⁷³ См.: Курс А. Элемент интереса в информации // Журналист. 1928. № 1. С. 43.

оригинальность фактов являлись основными признаками понятия информации.

После попытки качественного (содержательного) осмысления исследуемого понятия гуманитарными науками, изучением его количественных признаков занялась математика. Однако на фоне главной задачи (разработки способа количественного измерения информации), нередко математические теории информации касались и содержательной стороны исследуемого понятия.

Среди самых известных математических теорий информации можно выделить комбинаторную, вероятностно-статистическую, алгоритмическую и др.. В рамках математических теории не только разрабатывалось содержание понятия информации, но также определялись ее значимость, полезность, ценность и иные свойства, которые позднее использовались другими науками и отраслями права.

Важный вклад в теорию информации был внесен А.Н. Колмогоровым, который рассмотрел алгоритмический аспект этого явления. Он представлял количество информации как минимальную длину программы, позволяющую однозначно преобразовать один объект (множество) в другой (другое множество)¹⁷⁴. Кроме того, был расширен объем понятия информации, который стал включать в себя не только человеческую речь, но и любые объекты и процессы, подчиняющиеся статистическим закономерностям¹⁷⁵. Это положило начало изучению понятия информации кибернетикой. Ею был поднят забытый на некоторое время математическими теориями информации вопрос о ценности информации. А.А. Харкевич считал, что «...ценность может измеряться через приращение вероятности достижения цели до и после получения информации»¹⁷⁶. Это свидетельствует о том, что выводы о

¹⁷⁴ См.: Колмогоров А.Н. Три подхода к определению понятия «количество информации» // Проблема передачи информации. 1965. Т. 1, Вып. 1. С. 3-11.

¹⁷⁵ См.: Григорьев А.Н. Информация и информационное взаимодействие в расследовании преступлений: теоретические аспекты. Калининград: Калининградский ЮИ МВД России, 2006. С. 14.

¹⁷⁶ См.: Урсул А.Д. Природа информации: философский очерк. Челябинск, 2010 [Электронный ресурс]. URL: http://www.inion.ru/files/File/Ursul_A_D_Priroda_informacii.pdf (дата обращения: 28.05.2016).

содержании понятия «информационной ценности» из журналистики (А. Курс) перешли в кибернетику. То есть из социальной сферы – в сферу управления.

Качественные признаки информации подверглись научному осмыслению в работах А.С. Пресмана. Он определял информацию как характеристику организованности систем. Чем сложнее система, отмечал автор, тем ярче проявляется качественный характер информации¹⁷⁷.

Становление понятия информации в кибернетике связано также с именем философа Н. Винера. Он проанализировал соотношение понятий информация и управление, которое является центральным в кибернетике. Согласно ему, управление – это «...процесс переработки (преобразования) информации, получаемой от источников информации (сенсорных рецепторов), и передачи ее в те участки системы, где она воспринимается ее элементами как приказ для выполнения того или иного действия»¹⁷⁸. Таким образом, информация понимается как некоторая величина, над которой совершаются процессы переработки (преобразования), то есть действия.

Представители семантической теории возвращают нас к содержательной стороне информации. Например, согласно теории Р. Карнапа и Й. Бар-Хиллела информацией признавались лишь те сведения, которые являлись принципиально новыми по сравнению с имеющимися у человечества знаниями¹⁷⁹.

Вышеизложенный анализ понятия информации, являющейся предметом изучения многих наук, доказывает определенную закономерность. Она связана с зависимостью интеграции понятия в новые сферы научного знания и расширением значимых свойств этого понятия.

¹⁷⁷ См.: Пресман А.С. Организация биосферы и ее космические связи. М.: Гео-Синтег, 1997. С. 26-27.

¹⁷⁸ См.: Wiener N. Cybernetics (first edition 1948). Cambridge: MIT Press, 1961. P. 10.

¹⁷⁹ См.: Урсул А.Д. Природа информации. Философский очерк. М.: Политиздат, 1968. С.48-51.

Как писал Ф. Энгельс понятия необходимо рассматривать «...в их историческом, соответственно – логическом, процессе образования»¹⁸⁰.

Проведенный нами анализ поможет осмыслить и выявить основные признаки понятия информации на современном этапе развития права.

Согласно Федеральному закону Российской Федерации № 149-ФЗ от 27.07.2006 года (с изм. и доп. от 06.07.2016) «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон от 27.07.2006 № 149-ФЗ) под информацией понимаются «...сведения (сообщения, данные) независимо от формы их представления»¹⁸¹. С момента вступления в силу вышеназванного Федерального закона от 27.07.2006 № 149-ФЗ ведутся споры, касающиеся такого содержания данного понятия.

Заметим, что информация, как правовая категория, законодательно раскрывается довольно-таки размыто, однако говорить о том, что это является безусловным недостатком, однозначно нельзя. Так, понятие имущества как объекта гражданского права имеет более широкое толкование, нежели чем понятие имущества как предмета хищения в УК РФ. Когда мы говорим о понятийном аппарате закона, имеющем широкую направленность, раскрывающем суть специфичных отношений, вопросами регулирования и охраны которых занимаются различные отрасли права, то он должен быть не узконаправленным, в связи с чем полагаем, что нет необходимости вносить какие-либо изменения в понятие информации, предусмотренное Федеральным законом от 27.07.2006 № 149-ФЗ. Более тщательно и подробно необходимо проработать понятие информации, используемое в гражданском, административном и уголовном законодательстве.

¹⁸⁰ См.: Маркс К. Капитал: критика политической экономии. Т. 3. Книга III. Процесс капиталистического производства, взятый в целом / под ред. Ф. Энгельса [Электронный ресурс]. URL: <http://www.esperanto.mv.ru/Marksismo/Kapital3/kapital3-00.html> (дата обращения: 10.05.2016).

¹⁸¹ См.: Федеральный закон от 27.07.2006 № 149-ФЗ (с изм. и доп. от 06.07.2016, № 374-ФЗ) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.), ст. 3448; 2016. № 28, ст. 4558.

Гражданское право некоторое время выделяло в качестве своего объекта информацию, в частности, имелась в виду информация, содержащая коммерческую или служебную тайну (то есть, если обратиться к Федеральному закону от 27.07.2006 № 149-ФЗ, – документированная информация¹⁸²). Однако вышеназванные положения Гражданского кодекса Российской Федерации (далее – ГК РФ) ныне утратили силу¹⁸³. Хотя в ГК РФ информация уже не входит в перечень объектов гражданских правоотношений согласно ст. 128 и 139 ГК РФ (часть первая ГК РФ), это вовсе не означает, что вопросы, связанные с хранением, передачей и иным использованием информации, не относятся в том числе и к гражданско-правовым. В ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ закреплено, что информация может являться объектом публичных, гражданских и иных правовых отношений. Круг таких отношений не исчерпывающий. Кроме того, за нарушение законодательства, связанного с защитой информации, может возникнуть дисциплинарная, гражданско-правовая, административная и даже уголовная ответственность.

Понятия «информация», «сведения», «сообщения», «данные» являются часто используемыми, а некоторые – взаимозаменяемыми в ГК РФ. Так, содержание ст. 152 ГК РФ направлено на защиту чести, достоинства или деловой репутации граждан. В частности, часть 4 регламентирует случаи, когда сведения, порочащие честь, достоинство или деловую репутацию, стали широко известны, в связи с этим опровержение невозможно донести до всеобщего сведения. В таком случае гражданин имеет право требовать удаления такой информации (то есть сведений, порочащих честь, достоинство или деловую репутацию). В той же главе 8 ГК РФ («нематериальные блага и их защита») содержание ст. 152.2 направлено на

¹⁸² Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

¹⁸³ См.: Федеральный закон от 18.12.2006 № 231-ФЗ (с изм. и доп. от 01.07.2015, № 476-ФЗ) «О введении в действие части четвертой Гражданского кодекса Российской Федерации» // СЗ РФ. 2006. № 52 (ч.1), ст. 5497; 2015. № (ч.1), ст. 29.

обеспечение охраны частной жизни граждан, а именно: «...не допускаются без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства...».

Статья 727 ГК РФ регламентирует вопросы, связанные с обеспечением конфиденциальности информации, полученной сторонами договора подряда. Так, если сторона благодаря исполнению своего обязательства получила от другой стороны информацию о новых решениях и технических знаниях, а также сведения, в отношении которых их обладателем установлен режим коммерческой тайны, сторона, получившая такую информацию не вправе сообщать ее третьим лицам. Таким образом, ГК РФ также как и Федеральный закон от 27.07.2006 № 149-ФЗ, раскрывает понятие информации в том числе и через понятие сведений (см. также ч. 3 ст. 1350 ГК РФ).

Понятие «данные» в ГК РФ часто используется применительно к недвижимому имуществу: данные о государственной регистрации (ст. 60, 63 ГК РФ); данные, позволяющие определенно установить недвижимое имущество, подлежащее передаче покупателю (арендатору) по договору (ст. 554, 607 ГК РФ). Однако практически все значения, в которых используется понятие «данные» в ГК РФ теоретически можно заменить понятиями информации или сведений. Раздел VII ГК РФ (часть четвертая) регламентирует положения, связанные с использованием результатов интеллектуальной деятельности и средств индивидуализации. В частности ч. 4 ст. 1243 ГК РФ регулирует отношения, связанные с использованием объектов авторских и смежных прав на основе сведений и документов, получаемых от пользователей, а также других данных об использовании объектов авторских и смежных прав, в том числе сведений статистического характера. Таким образом, законодатель использует в качестве взаимозаменяемых понятия «сведения» и «данные».

Понятие «сообщение» в тексте ГК РФ используется в разных значениях. Так, оно может употребляться в качестве формы, посредством

которой передается определенная информация. В таком случае оно является взаимозаменяемым к таким понятиям, как «заявление», «уведомление», «извещение», «требования». Тем самым, ГК РФ определяет сообщение как юридически значимую информацию. Но, как и в Федеральном законе от 27.07.2006 № 149-ФЗ, оно используется и как синоним понятия информации, а также как процесс (то есть определенное действие). Произведенный анализ всех четырех частей ГК РФ показал, что законодатель активно использует понятие информации, а также иные формы его выражения в качестве взаимозаменяемых – сведения, сообщения, данные.

Поскольку в настоящее время актуальной для законодательства является административная преюдиция как средство юридической техники, в правовом анализе понятия «информация» нельзя оставить без внимания Кодекс об административных правонарушениях Российской Федерации (далее – КоАП РФ). Наиболее активно законодателем используются понятия «информация» и «сведения», причем, как и в ГК РФ, встречаются статьи, в которых понятие информации заменяется понятием сведений, или наоборот.

Так, ч. 1 ст. 13.28 КоАП РФ устанавливает административную ответственность за нарушение порядка предоставления *информации* о деятельности государственных органов и органов местного самоуправления, содержащей *сведения*, относящиеся к *информации* ограниченного доступа. Статья 15.4 КоАП РФ предусматривает ответственность за нарушение срока представления *сведений* об открытии и о закрытии счета в банке или иной кредитной организации. Диспозиция же названной статьи звучит следующим образом: «нарушение установленного срока представления в налоговый орган *информации* об открытии или о закрытии счета в банке или иной кредитной организации». Статья 19.7 КоАП РФ устанавливает ответственность за непредставление *сведений (информации)*. В ст. 8.5 КоАП законодатель под сокрытием или искажением экологической *информации* понимает совершение различных действий, одними из которых являются: «искажение или несвоевременное сообщение полной и достоверной

информации о состоянии окружающей среды, о радиационной обстановке *данных*, полученных при осуществлении производственного экологического контроля, искажение *сведений* о состоянии земель...».

Более того, в административном законодательстве есть целая глава, посвященная защите информации – «административные правонарушения в области связи и информации».

Проведенный анализ позволяет сделать вывод о том, что законодатель в сфере административного права активно использует понятия информации и сведений, которые часто выступают в качестве предмета различных правонарушений.

Уголовное законодательство Российской Федерации (в отличие от гражданского или административного) не столь часто использует понятия информации, сведений, данных и сообщений. Однако, как было уже отмечено ранее, информация и иные формы ее выражения могут быть предметом некоторых преступлений. Кроме того, глава 28 УК РФ предусматривает ответственность за совершение преступлений в сфере компьютерной информации, где последняя раскрывается как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Таким образом сущность компьютерной информации основывается на понятии информации, которое дается в Федеральном законе от 27.07.2006 № 149-ФЗ.

Показательных примеров взаимозамены понятий «информация», «сведения», «сообщения», «данные» в УК РФ встретить сложно. Например, в ст. 195 УК РФ устанавливается ответственность за неправомерные действия при банкротстве, под которыми понимается в том числе: сокрытие имущества, имущественных прав или имущественных обязанностей, *сведений* об имуществе либо иной *информации* об имуществе. То есть понятие «сведения» включается в понятие «информация» в контексте данной диспозиции.

Существуют примеры неявного подразумевания под понятием «информация» понятия «сведения». Так, ч. 1 ст. 185³ УК РФ устанавливает ответственность за манипулирование рынком, то есть умышленное распространение заведомо ложных сведений или иные умышленные действия, запрещенные законодательством Российской Федерации о противодействии неправомерному использованию инсайдерской информации. При этом специализированный Федеральный закон от 27.07.2010 года № 224-ФЗ (ред. от 03.07.2016) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» под инсайдерской информацией понимает точную и конкретную информацию, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну)¹⁸⁴. Таким образом, положения специализированного законодательства позволяют определить, что представляет собой понятие инсайдерской информации, содержащейся в диспозиции ч. 1 ст. 185³ УК РФ.

Вышеназванные правовые акты: ГК РФ, КоАП РФ, УК РФ – используют в различном контексте все названные в Федеральном законе от 27.07.2006 № 149-ФЗ формы выражения понятия информации (сведения, сообщения, данные). Прослеживается тенденция использования каждой из названных форм в определенных устойчивых фразах, выражениях и законодательных понятиях. Так, для определения государственной тайны используется понятие сведений¹⁸⁵, что отражается также в Уголовном законодательстве, в частности в таких статьях как 275, 276, 283 УК РФ и т.д. Однако, в диспозиции ст. 13.12 КоАП РФ, устанавливающей ответственность

¹⁸⁴ См.: Федеральный закон от 27.07.2010 года № 224-ФЗ (с изм. и доп. от 03.07.2016, № 292-ФЗ) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2010. № 31, ст. 4193; 2016. № 27 (ч.1), ст. 4225.

¹⁸⁵ См.: Закон Российской Федерации от 21.07.1993 № 5485-1 (с изм. и доп. от 08.03.2015, № 23-ФЗ) «О государственной тайне» // СЗ РФ. 1997. № 41, ст. 8220-8235; 2015. № 10, ст. 1393.

за нарушение правил защиты информации, используется такое словосочетание как «информация, составляющая государственную тайну», то есть вместо понятия «сведения» используется понятие «информация».

С одной стороны это допустимо, учитывая, что сам уже не раз упоминаемый Федеральный закон от 27.07.2006 № 149-ФЗ позволяет раскрывать понятие информации через синонимичные ему – сведения, сообщения и данные. Более того, такая тенденция прослеживается и в толковых словарях русского языка.

Так, согласно Толковому словарю русского языка С.И. Ожегова и Н.Ю. Шведова под *информацией* понимаются «сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством»¹⁸⁶. Такая трактовка характерна для кибернетического понимания информации. Понятие «сведения» раскрывается через несколько значений, одними из которых являются: 1) познания в какой-либо области; 2) известие, *сообщение*¹⁸⁷. Под *сообщением* понимается «то, что сообщается, известие, *информация*», но в первую очередь словарь для установления содержания этого понятия отправляет нас к понятию «сообщить», то есть к процессу, действию¹⁸⁸. Под *данными* же понимаются «сведения, необходимые для какого-нибудь вывода, решения»¹⁸⁹.

В лексикографии (разделе языкознания, занимающемся вопросами составления словарей) устанавливается, что при трактовке понятий в толковых словарях используются близкие по значению слова (синонимы). Однако, как отмечают специалисты в области синонимии, «близость» таких понятий определяется в тождестве их отдельных значений¹⁹⁰, то есть заменить понятие близким по значению возможно не в каждом контексте.

¹⁸⁶ См.: Ожегов С. И., Шведов Н.Ю. Толковый словарь русского языка (4-е изд. доп.). М.: Азбуковник, 1999. С. 250.

¹⁸⁷ См.: Там же. С. 699.

¹⁸⁸ См.: Там же. С. 747.

¹⁸⁹ См.: Там же. С. 151.

¹⁹⁰ См.: Бережан С.Г. К Семасиологической интерпретации явления синонимии. См.: Лексическая синонимия (сборник статей) // под ред. С.Г. Бархударова. М.: Наука, 1967. С. 45.

Очевидно, что законодатель за основу понятия информации в Федеральном законе от 27.07.2006 № 149-ФЗ взял положения, разработанные ранее гуманитарными науками, что может быть допустимым. Однако существуют правила юридической техники, которые подразумевают необходимость избегать двусмысленности в понимании юридических и иных понятий, используемых в правовых актах. Это обусловлено тем, что только однозначность понятийного аппарата может стать основанием для формирования эффективных правовых норм, регулирующих отношения в информационной сфере¹⁹¹.

Вышеизложенное обосновывает необходимость в разработке единых условий взаимозаменяемости и использования понятия информации и иных синонимичных форм ее выражения (сведений, сообщений, данных) в определенных правовых контекстах.

Федеральный закон от 27.07.2006 № 149-ФЗ не дает разъяснения о характерных признаках информации как сведений (сообщений, данных). Это позволяет сделать вывод о том, что в рамках данного закона информация понимается в самом широком смысле. Однако в связи с тем, что информация может являться предметом и средством («орудием») совершения преступления, необходимо установить признаки, которые прежде всего обнаруживают себя в случаях использования ее для совершения общественно-опасных деяний, в том числе для совершения преступлений и правонарушений террористической направленности.

На доктринальном уровне уже предпринимались попытки формирования признаков охраняемой государством официальной информации как нуждающейся в особой правовой защите¹⁹², а также информации, являющейся предметом или средством совершения

¹⁹¹ См.: Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник. СПб.: Юридический центр Пресс, 2001. С. 80-81.

¹⁹² Признаками охраняемой государством официальной информации являются: 1) это сведения о фактах, имеющих юридическое значение; создание ее уполномоченным государством производителем (физическим или юридическим лицом); подчинение ее особому правовому режиму. См.: Букалерева Л.А. Указ. соч. С. 90-92.

преступлений в сфере экономической деятельности¹⁹³. Однако правовому анализу в научных исследованиях подвергалась лишь часть информации, а именно – находящаяся в системе управленческих официальных отношений либо отношений, складывающихся в сфере экономической деятельности. Для целей же настоящего диссертационного исследования необходимо выделить признаки информации, которая может стать предметом или средством («орудием») именно террористических преступлений. К таковым признакам, по нашему мнению, необходимо относить следующие:

1. *Информация есть сведения.* Проведенный анализ правовых норм ГК РФ, КоАП РФ, УК РФ позволяет сделать вывод о том, что понятие информации чаще всего в законодательстве раскрывается через понятие сведений. Причем, как отмечает С.А. Яшков (и с чем, по нашему мнению, следует согласиться), понятия «информация» и «сведения» являются тождественными, полностью совпадающими в правовом контексте¹⁹⁴. Другие же понятия – «сообщения» и «данные» – являются синонимичными по отношению к понятию информации, совпадающими лишь в определенной части¹⁹⁵.

2. *Информация это сведения, обладающие информационной ценностью,* то есть имеющие значение для достижения определенного преступного результата. Преступник, в первую очередь, должен осознавать значимость таких сведений. В других научных исследованиях данный признак информации, как правовой категории, определяется следующим образом: «наличие связи между информацией и ее потребителем»¹⁹⁶.

¹⁹³ См.: Турьшев А.А. Информация как признак преступлений в сфере экономической деятельности: дис. ... канд. юрид. наук. Омск, 2006. С. 180.

¹⁹⁴ См.: Яшков С.А. Информация как предмет преступления: дис. ... канд. юрид. наук. Екатеринбург, 2005. С. 39.

¹⁹⁵ Через «сведения» раскрывает понятие информации как предмета экономических преступлений и Р.Г. Асланян. См.: Асланян Р.Г. Информация как предмет и средство совершения преступления в сфере экономической деятельности: дис. ... канд. юрид. наук. Краснодар, 2016. С. 33.

¹⁹⁶ См.: Яковлева И.А. Информация с ограниченным доступом в предпринимательской деятельности: правовой аспект: автореф. дис. ... канд. юрид. наук. М., 2014. С. 16; Салихов И.И. Информация с ограниченным доступом как объект гражданских правоотношений: автореф. дис. ... канд. юрид. наук. Казань, 2004. С. 11.

3. *Информация находится на определенных носителях*¹⁹⁷. Информация не может существовать вне знаковых или языковых систем¹⁹⁸. Это могут быть самые разнообразные материальные носители (машинный, бумажный, компьютерный, аудио-, видеоноситель и другие), а также сам человек, память которого позволяет хранить и передавать информацию другим субъектам¹⁹⁹.

4. *Использование информации как предмета или средства («орудия») для достижения преступных целей.* Такая цель может проявляться в следующем:

- в запугивании населения либо в оказании психологического воздействия (например, проникновение в электронную систему SCADA штата Иллинойс, что вызвало перебои в водоснабжении²⁰⁰; до 2008 г. на территории Шри-Ланки действовала радиостанция «Тигров освобождения Тамил Илама», на частотах которой распространялась идеология, присущая террористам, и публичные призывы к осуществлению террористической деятельности²⁰¹);

- в совершении или в облегчении совершения другого преступления (например, убийство иранского физика-ядерщика с помощью информации, которой располагало Международное агентство по атомной энергии (МАГАТЭ)²⁰²);

- в изменении политических взглядов населения или какой-либо социальной группы, о чем свидетельствуют некоторые социологические исследования по вопросам противодействия терроризму²⁰³;

¹⁹⁷ См.: Салихов И.И. Информация с ограниченным доступом как объект гражданских правоотношений: дис. ... канд. юрид. наук. Казань, 2004. С. 21; Букалерева Л.А. Указ. соч. С. 87-89.

¹⁹⁸ См.: Салихов И.И. Указ. соч. С. 21.

¹⁹⁹ См.: Букалерева Л.А. Уголовно-правовая охрана человека как носителя информации // Уголовное право: стратегия развития в XXI веке. сб. материалов третьей Международной научно-практической конференции. М., 2006. С. 151-154.

²⁰⁰ См.: Хакеры взломали SCADA-систему одной из американских ГЭС [Электронный ресурс]. URL: <http://www.securitylab.ru/news/410200.php> (дата обращения: 14.04.2016).

²⁰¹ См.: BBC Шри-Ланки разбомбили радио «тамилских тигров» // [Электронный ресурс]. URL: <https://lenta.ru/news/2007/11/27/station/> (дата обращения: 11.05.2016).

²⁰² См.: Бондарь Ю.М. Иран: январь 2012 г. Военно-политическая ситуация // Институт Ближнего Востока [Электронный ресурс]. URL: <http://www.iimes.ru/rus/stat/2012/27-02-12d.htm> (дата обращения: 12.04.2016).

²⁰³ См.: Обобщенные результаты социологического исследования по вопросам противодействия идеологии терроризма в 2012 году [Электронный ресурс]. URL: <http://scienceport.ru/files/soc-isledovaniya-2012.pdf> (дата обращения: 14.06.2015).

Некоторый спор возникает по поводу того, является ли качественная (содержательная) сторона необходимым атрибутом информации. С.А. Яшков полагает, что существенным свойством информации является лишь то, что это – сведения²⁰⁴. Другие же признаки: целевое назначение, актуальность, адекватность, достаточность и др. – являются лишь факультативными²⁰⁵. Однако подавляющее большинство ученых выделяют качественную характеристику как существенный признак информации²⁰⁶.

Исходя из вышеизложенного *информация, как предмет или средство («орудие») преступления, – это сведения, находящиеся на определенном носителе, обладающие информационной ценностью для своего потребителя или пользователя, использование которых необходимо для достижения преступных целей.*

Представляется возможным определить некоторые общественно-опасные деяния террористического характера, связанные с использованием информации в качестве их предмета или средства («орудия») совершения:

- 1) кибернетические (компьютерные) преступления (к которым, в частности, относят преступления, содержащиеся в гл. 28 УК РФ);
- 2) дезинформацию, направленную на запугивание (устрашение) населения, изменение политических взглядов какой-либо социальной группы и т.п.²⁰⁷;
- 3) незаконное использование и (или) создание, и (или) руководство СМИ с целью психологического воздействия на население или какую-либо социальную группу;
- 4) пропаганду как акт психологического воздействия²⁰⁸;
- 5) вовлечение, склонение или вербовку физических лиц к совершению преступлений (правонарушений) террористического характера;

²⁰⁴ См.: Яшков С.А. Указ. соч. С. 8.

²⁰⁵ См.: Там же. С. 46.

²⁰⁶ См.: Яковлева И.А. Указ. соч. С. 16; Салихов И.И. Указ. соч. С. 11; Букалерева Л.А. Указ. соч. С. 90-91.

²⁰⁷ См.: Столяров А.В. Информационная свобода и информационное насилие: дис. ... канд. философ. наук. М., 2012. С. 41.

²⁰⁸ См.: Там же. С. 41.

б) публичные призывы к осуществлению террористической деятельности и публичное оправдание терроризма;

в) другие способы использования террористами информации для совершения преступлений.

Названные и подобные им по содержанию преступления есть основания относить к информационному терроризму при наличии присущих последнему признаков.

Помимо информации средствами (инструментами) информационного воздействия выступают также информационные технологии и информационные ресурсы.

В настоящее время информационные технологии активно используются сферой образования, здравоохранения, экономики и т.п. Возросший интерес к ним и относительная доступность не остались без внимания и правонарушителей. Федеральным законом от 27.07.2006 № 149-ФЗ информационные технологии определяются как процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Таким образом, в самом широком смысле к ним следует относить различные компьютерные и иные программы, созданные и используемые различными средствами вычислительной техники, информационно-телекоммуникационную сеть (Интернет и иную локальную или территориальную сеть), различные средства вычислительной техники (технические устройства) и т.п.²⁰⁹, необходимые для создания, хранения, управления, передачи и поиска *электронной*²¹⁰ информации²¹¹.

²⁰⁹ Понятия «информационные технологии» и «компьютерные технологии» совпадают лишь в определенной части. Научному миру известны и некомпьютерные информационные технологии. См.: Минькович Т.В. Информационные технологии: понятийно-терминологический аспект // Образовательные технологии и общество. 2012. № 2. Том 15. С. 383-384.

²¹⁰ Считаю необходимым использовать при раскрытии содержания понятия информационных технологий понятие электронной информации, которое является более широким, нежели понятие компьютерной информации. См.: Кушниренко С.П. Цифровая информация как самостоятельный объект криминалистического исследования [Электронный ресурс]. URL: <http://www.law.edu.ru/doc/document.asp?docID=1311821> (дата обращения: 12.05.2016).

²¹¹ См.: Толковый словарь терминов понятийного аппарата информатизации образования / сост. И.В. Роберт, Т.А. Лавина. М.: ИИО РАО, 2009. С. 13; Минькович Т.В. Указ. соч. С. 377.

На сегодняшний день содержащееся в Федеральном законе от 27.07.2006 № 149-ФЗ понятие информационных технологий требует более детального разъяснения, поскольку возникают трудности при отнесении тех или иных процессов, методов поиска, сбора информации к таковым, тем более что за последние несколько лет законодательство в этой части претерпевало определенные изменения, что обусловлено использованием информационных технологий в целях совершения преступлений (правонарушений) в различных сферах.

Сегодня использование, в частности, информационно-телекоммуникационных сетей (в том числе сети Интернет)²¹² является квалифицирующим или особо квалифицирующим признаком некоторых составов преступлений против здоровья населения и общественной нравственности (например, ст. 242 – 242² УК РФ), основ конституционного строя и безопасности государства (например, ст. 280, 280¹, 282 УК РФ). Использование информационных технологий упрощает совершение преступлений (например, ст. 159⁶ УК РФ), переводит их на новую, более безопасную для преступника платформу действия – информационное пространство.

По аналогии с УК РФ, КоАП РФ устанавливает в качестве особого признака использование информационных технологий (информационно-телекоммуникационных сетей) для некоторых составов правонарушений, посягающих на здоровье, санитарно-эпидемиологическое благополучие населения и общественную нравственность, в области связи и информации и так далее. Также как и в УК РФ, КоАП РФ устанавливает ответственность за правонарушения, где новой платформой их осуществления стало информационное пространство, а также за относительно новые правонарушения, осуществляемые исключительно в пределах информационного пространства (глава 13 КоАП РФ).

²¹² Понятие «информационно-телекоммуникационная сеть» (в том числе сеть Интернет) как признак некоторых составов преступлений и правонарушений является составляющим понятия «информационные технологии». См.: Минькович Т.В. Указ. соч. С. 385.

Кроме того, информационные технологии могут являться средством организации и координации деятельности террористов при совершении террористического акта. Так, по данным некоторых российских СМИ для координации деятельности террористического акта во Франции были использованы игровые приставки PlayStation 4, отследить передачу данных по которым очень сложно²¹³. Кроме того, сервис мгновенной передачи сообщений Telegram используется террористической организацией ИГИЛ для пропаганды и вербовки новых членов²¹⁴.

Еще одним инструментом совершения преступлений или правонарушений в информационной сфере выступают информационные ресурсы. В ранее действующем Федеральном законе РФ № 24-ФЗ от 20.02.1995 «Об информации, информатизации и защите информации»²¹⁵ под информационными ресурсами понимались документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Такое содержание исследуемого понятия можно было признать приемлемым, однако исследователи²¹⁶ указывали на отсутствие некоторых очень важных его признаков. К таковым, в частности, следует относить:

- 1) информационные ресурсы – это информация, организованная соответствующим образом;
- 2) формами ее организации выступают: библиотеки, архивы, фонды, банки данных, информационные системы²¹⁷;
- 3) минимальной единицей исследуемого понятия выступает документ²¹⁸ (однако данной позиции противостоит мнение некоторых

²¹³ См.: Парижские террористы использовали для связи PlayStation 4 [Электронный ресурс]. URL: <http://rsute.ru/obshchestvo/51625.html> (дата обращения 17.11.2015).

²¹⁴ См.: Ермаков Г. Telegram содержит 30-40 каналов ИГИЛ, используемых террористами для пропаганды [Электронный ресурс]. URL: <http://www.3dnews.ru/923839> (дата обращения: 11.05.2016).

²¹⁵ В настоящее время утратил юридическую силу.

²¹⁶ См.: Информационные ресурсы развития Российской Федерации: правовые проблемы / А.А. Антопольский, И.Л. Бачило, Г.В. Белов [и др.]; отв. ред. И.Л. Бачило. М.: Наука, 2003. С 26; Кривоухов А.А. Правовое регулирование защиты государственных информационных ресурсов: дис. ... канд. юрид. наук. Воронеж, 2006. С. 12.

²¹⁷ См.: Прокопенко А.Н. О содержании понятия информационные ресурсы в праве // Бизнес в законе. Экономико-юридический журнал. 2010. № 1. С. 159-160.

исследователей о возможности определения в качестве информационного ресурса чрезвычайно важную часть знаний, которой обладает человек – например, ученый, инженер, врач²¹⁹).

Соглашаясь с А.Н. Прокопенко, определим информационный ресурс как организованную и структурированную документированную информацию, содержащуюся в библиотеках, архивах, фондах, банках данных, информационных системах²²⁰.

Все вышеизложенное свидетельствует о следующем:

1) при столь широком определении понятия информации следует разработать условия по его взаимозаменяемости с другими сходными по значению понятиями («сведения», «сообщения», «данные») в рамках действующего законодательства;

2) информация как предмет или средство («орудие») преступления – это сведения, находящиеся на определенном носителе, обладающие информационной ценностью для своего потребителя или пользователя, использование которых необходимо для достижения преступных целей.

3) понятие информационных технологий в Федеральном законе от 27.07.2006 № 149-ФЗ следует раскрывать как процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения *электронной* информации и способы осуществления таких процессов и методов. Кроме того, необходимо определить примерный перечень таких процессов, методов поиска, сбора, хранения электронной информации для наиболее правильного применения норм специализированного законодательства, регламентирующего вопросы использования или воздействия на информационные технологии.

²¹⁸ См.: Солдаткина О.Л. Информационные ресурсы российской правовой политики: общетеоретический аспект: дис. ... канд. юрид. наук. Саратов, 2001. С. 38.

²¹⁹ См.: Курс «Мировые информационные ресурсы» [Электронный ресурс]. URL: <http://mir.it-karma.ru/teoreticeskie-osnovy-informacionnyh-resursov/lekcii/1-osnovnye-ponatia-i-susnost-informacionnyh-resursov> (дата обращения: 26.05.2016).

²²⁰ См.: Прокопенко А.Н. Указ. соч. С. 160.

4) следует согласиться с содержанием понятия информационные ресурсы, предложенным А.Н. Прокопенко, и определять его как организованную и структурированную документированную информацию, содержащуюся в библиотеках, архивах, фондах, банках данных, информационных системах.

§3. Виды информационного терроризма

В связи с возникновением сети Интернет произошло глобальное расширение информационного пространства. Это привело к возникновению новых форм законной и противоправной деятельности.

На сегодняшний день исследователями уже не раз отмечалась возрастающая опасность негативного воздействия информации на психику людей²²¹. Ранее анализируемый Проект Конвенции об обеспечении международной информационной безопасности определяет в качестве основных угроз международному миру и безопасности в информационном пространстве дезинформацию и сокрытие информации с целью искажения духовной и психологической среды общества²²². На одном из заседаний Совета Федерации по вопросам защиты информационного пространства оценивалась проблема усиливающегося информационно-пропагандистского влияния терроризма²²³. Террористические угрозы в информационном пространстве связывают с информационно-психологическим воздействием на сознательно-волевые компоненты личности, социальной группы, общества, субъектов власти, представителей иностранных государств и международных организаций и т.п. Кроме того, в рамках новой сферы информационного пространства – киберпространства, – возникла угроза воздействия на отдельные элементы информационной среды²²⁴ государств, международных организаций (в том числе инфраструктуры).

²²¹ См.: Ежевская Т.И. Психологическое воздействие информационной среды на современного человека // Психопедагогика в правоохранительных органах. 2009. № 2. С. 89; Информационные вызовы национальной и международной безопасности / под общ. ред. А.В. Федорова, В.Н. Цыгичко. М.: ПИР-Центр, 2001. С. 56.

²²² См.: Проект Конвенции об обеспечении международной информационной безопасности (концепция) [Электронный ресурс]. URL: <http://www.scrf.gov.ru/documents/6/112.html> (дата обращения: 12.05.2016).

²²³ См.: В Совете Федерации обсудили проблему информационного терроризма // Наука и образования против террора [Электронный ресурс]. URL: <http://scienceport.ru/anlytics/v-sovete-federatsii-obsudili-problemu-informatsionnogo-terrorizma/> (дата обращения: 12.05.2016).

²²⁴ Информационная среда – это совокупность информационных систем, информационной инфраструктуры, других средств, обеспечивающих порождение, перемещение, хранение, обработку и представление информации, носителей информации. См.: Энциклопедия информационного общества [Электронный ресурс]. URL: http://wiki.iis.ru/wiki/Информационная_среда (дата обращения: 27.05.2016).

Следует признать правильной точку зрения некоторых ученых о том, что детальное исследование проблемы противодействия информационному терроризму, возможно лишь путем выделения его видов²²⁵. Соглашаясь в этом вопросе с такими исследователями, как А.И. Маляров, В. Цыганов, А.И. Примакин, В.Е. Кадулин, Ю.И. Жуков, В.И. Антюхов²²⁶, считаем необходимым выделять такой вид информационного терроризма (в зависимости от средств воздействия и объектов такого воздействия), как *информационно-психологический терроризм*.

Психологический компонент всегда сопровождал явление терроризма. Это выражается в первую очередь в определении устрашения как сущностного признака терроризма. Однако исследователями отмечается значительное повышение роли психологического воздействия, нередко выступающего самостоятельным инструментом террористической деятельности. В качестве участников информационно-психологического противоборства Э.И. Скакунов называет в том числе и организации религиозного, экстремистского, террористического толка²²⁷.

На сегодняшний день информационно-психологическое воздействие террористических групп (организаций или сообществ) осуществляется двумя способами:

- 1) опосредованно (СМИ усугубляют общественный страх гипертрофированными сообщениями, чрезмерным привлечением внимания к террористическим актам и характеристикам личности террористов);
- 2) непосредственно (создание террористическими группами (организациями или сообществами) своих веб-сайтов, СМИ, радио- и телевизионных частот для распространения пропаганды, дезинформации, а равно вовлечения, склонения, вербовки и призывов к осуществлению террористической деятельности, оправдания терроризма и т.п. лично, с

²²⁵ См.: Цыганов В. Указ соч. С. 24.

²²⁶ См.: Маляров А.И. Указ. соч. С. 4; Цыганов В. Указ. соч. С. 24-25; Примакин А.И., Кадулин В.Е., Жуков Ю.И., Антюхов В.И. Указ. соч. С. 57-58.

²²⁷ См.: Скакунов Э.И., Насиновский В.Е. Политические конфликты в современных условиях // США: экономика, политика, идеология. 1995. № 4. С. 11.

помощью сети Интернет либо иной информационно-телекоммуникационной сети)²²⁸.

1. Опосредованное воздействие.

Если раньше существование различных СМИ было необходимо для своевременного достоверного распространения информации, сейчас отмечается расширение их роли, направленной на формирование общественного сознания²²⁹. Так, представители североамериканской политологической науки называют среди прочих и такую функцию СМИ, как «формирование общественного мнения»²³⁰. Немного иначе называют эту функцию российские ученые: «СМИ как средство формирования реальности»²³¹. Безусловно, возможности СМИ, связанные с оперативностью, быстротой и масштабностью привлекаемой аудитории, не остались без внимания террористов. Неслучайно многие исследователи называют публичность, гласность и общественный резонанс²³² в качестве существенных признаков терроризма, что обусловлено опосредованным усилением СМИ обстановки страха.

Итак, деятельность СМИ, связанная с опосредованным информационно-психологическим воздействием, проявляется в *нагнетании отношений, сложившихся между различными социальными группами*.

Идеологическая основа современного терроризма довольно часто связана с межнациональными, межконфессиональными и межэтническими противоречиями. Объединяя в своих репортажах происшествия и определенные социальные группы, СМИ на подсознательном уровне формируют чувство страха и ненависти к такой группе.

²²⁸ См.: Федорова О.Н. Роль информационно-психологической безопасности граждан в России // Гуманитарные и социальные науки. 2012. № 2. С. 350.

²²⁹ См.: Голубин Р.В., Грачев С.И. Место средств массовой коммуникации в борьбе с терроризмом // Вестник Нижегородского университета им. Н.И. Лобачевского. 2007. №. 3. С. 218; Петришев В.Е. Заметки о терроризме. М.: Эдиториал УРСС, 2001. С. 108.

²³⁰ См.: Graber P.A. Mass Media and American Politics (5-th Ed.). Washington, 2000. P. 5–55.

²³¹ См.: Назаров М.М. Массовая коммуникация в современном мире: методика анализа и практика исследований. М.: УРСС, 2000. С. 7.

²³² См.: Гаврилин Ю.В., Смирнов Л.В. Современный терроризм: сущность, типология, проблемы противодействия: учебное пособие. М.: ЮИ МВД России, Книжный мир, 2003. С. 9.

Освещая события (в особенности – террористические акты), СМИ акцентируют либо усложняют и так непростые отношения между различными социальными объединениями. По мнению С.Н. Мещеряковой осуществляется это двумя основными методами:

- прямого и открытого действия, когда СМИ явно, не скрывая своих целей, нагнетают и обостряют эти отношения;
- «затрагивания»²³³.

В Российской Федерации свобода массовой информации гарантируется Конституцией, цензура запрещается. При этом не допускается пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства. Такие международные правовые акты, как Всеобщая декларация прав человека²³⁴, Международный пакт о гражданских и политических правах²³⁵, Американская конвенция о правах человека²³⁶, Европейская конвенция о правах человека²³⁷ и др. обеспечивают защиту прав на свободу выражения мнений на международном уровне.

Несмотря на такую мощную защиту фундаментальных демократических ценностей, в 2001 году в связи с терактом в США Д. Бушу пришлось запретить трансляцию любых заявлений Усамы бен Ладена, Аль-Каиды и руководителей «Талибана», что было воспринято журналистами как нарушение свободы слова. Д. Буш ответил, что пропаганда, каковой являются заявления данных лидеров, не может считаться законным

²³³ Названные методы могут проявляться в создании негативного образа какой-либо социальной, этнической либо религиозной группы; преувеличении масштаба реальной межнациональной, межконфессиональной проблемы либо конфликта между другими социальными группами; повышении эмоционального уровня проблемы; привязывании проблемы сложившегося конфликта к другим острым социальным трудностям и т.п. См.: Мещерякова С.Н. Российские средства массовой информации в институционально-правовом обеспечении межнационального согласия: дис. ... канд. юрид. наук. Ростов-на-Дону, 2005. С. 55-56.

²³⁴ См.: Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН) от 10 декабря 1948 // Рос. газета. 1995. 05 апр.

²³⁵ См.: Международный пакт о гражданских и политических правах от 16 декабря 1966 // Бюллетень Верховного Суда РФ. N 12. 1994.

²³⁶ См.: Американская конвенция о правах человека от 22 ноября 1969 [Электронный ресурс]. URL: <http://hrlibrary.umn.edu/russian/instree/Rzoas3con.html> (дата обращения 03.05.2016).

²³⁷ См.: Конвенция о защите прав человека и основных свобод от 4 ноября 1950 // СЗ РФ. 2001. N 2, ст. 163.

распространением информации²³⁸. При этом он ссылаясь на запрет всякой пропаганды войны, национальной, расовой и религиозной нетерпимости, закрепленный в международно-правовых актах, рассмотренных нами выше.

Вопросы обеспечения свободы массовой информации, а также установления ограничений (хотя бы этических) по злоупотреблению такой свободой являются сложными и дискуссионными. Это в первую очередь связано с тем, что свобода массовой информации выступает одним из элементов демократического идеала. Однако, как отмечает В.А. Поздняков, СМИ часто подменяет функцию передачи объективной информации, навязывая читателям (зрителям) мнение некоего автора или того, кто стоит за этим автором или изданием в целом²³⁹. Заметим, что на многих сайтах сети Интернет, признанных в соответствии с действующим законодательством РФ СМИ, размещение репортажей о каком-либо событии журналистом сопровождается отметкой, что данное СМИ не несет ответственности за сведения, предоставляемые им²⁴⁰.

Проблема освещения террористических актов и нагнетания обстановки непосредственно после их совершения. К опосредованному информационно-психологическому воздействию можно отнести также проблему освещения террористических актов СМИ. Российский военный аналитик В. Васильев, редактор «Армейского радио» в Израиле Н. Шелл акцентируют внимание на необходимости более нравственного и сдержанного освещения террористических актов без нагнетающих и драматических фраз²⁴¹.

Как писал Э. Фромм: для того чтобы миллионы поставили на карту свою жизнь и стали убийцами, им необходимо внушить такие чувства как

²³⁸ См.: Василенко В.В. Указ. соч. С. 100.

²³⁹ См.: Поздняков В.А. Философия культуры. М.: Интурреклама, 1999. С. 558.

²⁴⁰ На необходимость установления морально-этических норм освещения террористических актов и последующих событий указывали также Н.Ю. Лопаткин, Г.С. Чирков. См.: Лопаткин Н.Ю., Чирков Г.С. Организационно-правовые вопросы информационного противодействия терроризму в Российской Федерации // Вестник РГГУ. Серия: документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2011. № 18 (80). С. 274.

²⁴¹ См.: Почепцов Г.Г. Информационные войны. М.: Рефл-бук, К.: Ваклер, 2000. С. 218.

ненависть, возмущение и страх²⁴². Используемый журналистами язык вражды (*Hatespeech*) при характеристике личностей террористов формирует экстремистские начала в обществе. Например, после «Норд-Оста» был всплеск античеченских настроений, вызванных журналистами, а затем они сменились на неприязнь к «нерусским» вообще²⁴³.

После нескольких террористических актов в Волгограде, как отмечают специалисты, СМИ стали уделять пристальное внимание этнической и религиозной принадлежности предполагаемых террористов. Как полагает В.М. Амиров, СМИ, таким образом, «отказалось от моратория на откровенный анализ имеющихся в России национально-этнических противоречий»²⁴⁴. О проблемах освещения СМИ террористических актов, а также о необходимости их сбалансированного взаимодействия с властными структурами высказывались многие исследователи²⁴⁵.

Кроме того, анализ ситуации и выводы, которые делают СМИ России (особенно это относится к таким интернет-сайтам как, например, *zarusskiy.org*, *ruskline.ru*, *rusimperia.info* поддерживающим русских националистов), демонстрируют тенденцию ухудшения взаимоотношений с Северным Кавказом.

На сегодняшний день террористы благодаря СМИ не только формируют негативное отношение к себе, какой-либо социальной группе, что, по мнению некоторых исследователей, воспринимается ими как положительный результат своей деятельности, но и создают так называемый «лагерь сочувствующих»²⁴⁶. Нередко встречаются случаи косвенного оправдания террористов со стороны СМИ, что может выражаться в

²⁴² См.: Фромм Э. Душа человека. М.: ООО «Издательство АСТ»: ООО «Транзиткнига», 2004. С. 187.

²⁴³ См.: Семёнов З.Х. Особенности освещения явления «международный терроризм» в газетной периодике России: дис. ... канд. философ. наук. М., 2006. С. 170.

²⁴⁴ См.: Амиров В.М. Новые тенденции в освещении актов терроризма в российских печатных СМИ // Политическая лингвистика. 2014. № 1. С. 129.

²⁴⁵ См.: Колобов О.А., Сочнев Д.В., Шамов М.И. Информационный терроризм в современном российском обществе. Н. Новгород: Изд-во Нижегород. госуниверситета, 2007. С. 100-112.

²⁴⁶ См.: Великосельский М.Ю. Дискурс феномена терроризма в СМИ США: дис. ... канд. политич. наук. СПб., 2011. С. 93.

определении террористов как «борцов за свободу», подчеркивании их молодого возраста, символизации и т.п.²⁴⁷

Кроме того, благодаря СМИ террористы привлекают финансирование. В этой связи уместным будет использовать пример из истории, приведенный в одной из научных работ С. И. Грачевым и Р.В. Голубиным²⁴⁸. Пристальное внимание российских и зарубежных СМИ к деятельности чеченского полевого командира Хаттаба способствовало привлечению зарубежных спонсоров²⁴⁹.

Другая сторона деятельности СМИ предполагает *намеренное использование террористическими группами (организациями, сообществами) их всеобъемлющего влияния.*

Одной из функций СМИ, как отмечают некоторые ученые, является «фактор, способствующий приобретению известности»²⁵⁰. Потенциально огромная аудитория всего мира становится свидетелем террористической деятельности из-за СМИ и сети Интернет²⁵¹. Нет сомнений в том, что в настоящее время подавляющее большинство СМИ не направлено на сотрудничество с террористами для популяризации их деятельности. Однако в некоторых государствах находятся и такие²⁵², которые поддерживают терроризм. Так, один из сайтов «Хезболла» прямо обращается к журналистам, приглашая к сотрудничеству через электронную почту пресс-центра организации²⁵³.

Во время террористического акта 24 декабря 1994 года в Алжире, когда четыре террориста захватили рейсовый самолет с пассажирами (около 200

²⁴⁷ См.: Семёнова А.В., Корсунская М.В. Контент-анализ СМИ: проблемы и опыт применения / под ред. В.А. Мансурова. М.: Институт социологии РАН, 2010. С. 61-62.

²⁴⁸ См.: Голубин Р.В., Грачев С.И. Указ. соч. С. 219.

²⁴⁹ См.: Международный терроризм: борьба за геополитическое господство / под общ. ред. А.В. Возженикова. М.: РАГС, 2005. С. 306.

²⁵⁰ См.: Назаров М.М. Указ. соч. С. 7.

²⁵¹ См.: Шоткинов С.А. СМИ и преступность: специфика взаимодействия // Вестник Нижегородского университета им. Н.И. Лобачевского. 2003. № 1(6). С. 243.

²⁵² См.: Федорова О.Н. Указ. соч. С. 350; Белоножкин В.И., Остапенко Г.А. Информационные аспекты противодействия терроризму. М.: Горячая линия - Телеком, 2015. С. 12.

²⁵³ См.: Как современные террористы используют Интернет [Электронный ресурс]. URL: <http://www.alphagroup.kz/ru/media-files/stati/39-kak-sovremennye-terroristy-ispolzujut-internet> (дата обращения: 07.05.2016).

человек), в качестве антитеррористической операции им было предложено созвать пресс-конференцию. Террористы согласились и потребовали привести на борт журналистов агентства CNN²⁵⁴.

Как отмечает А.А. Робинов, свободный, не контролируемый поток информации все чаще используется радикальными, экстремистскими и террористическими организациями с целью захватить или подчинить своему влиянию СМИ²⁵⁵.

Ученые отмечают, что очень сложно проследить влияние СМИ на состояние преступности, однако у криминологов нет сомнений по поводу того, что одной из причин преступности могут выступать некоторые виды негативного воздействия СМИ на личность²⁵⁶. На сегодняшний день пособия по борьбе с терроризмом нередко упоминают о необходимости изолировать террористические группы от средств связи, в том числе от общения с журналистами, а также создать определенные ограничения на освещение, в частности, террористических актов²⁵⁷.

Опосредованное информационно-психологическое воздействие с помощью СМИ получило довольно широкое распространение и активно используется террористическими группами (организациями и сообществами).

Возникновение сети Интернет, развитие информационных технологий, выразившееся в создание новых технических устройств, способных прервать или перехватить трансляцию телевидения или радиочастот, способствовали развитию и другого направления деятельности террористических организаций. На сегодняшний день крупные международные террористические организации (сообщества) с продуманной системой

²⁵⁴ См.: Петров М.Н. Как уничтожить террористов. Действия штурмовых групп [Электронный ресурс]. URL: <http://coollib.com/b/266884> (дата обращения: 11.04.2016).

²⁵⁵ См.: Робинов А.А. Ограничение свободы СМИ и борьба с терроризмом // Журнал российского права. 2003. № 5. С. 104.

²⁵⁶ См.: Винецкий В.Н. Криминологические аспекты изучения современных средств массовой информации и их влияния на преступность // Вестник Воронежского института МВД России. 2011. № 4. С. 101.

²⁵⁷ См.: Петрищев В.Е. Указ. соч. С. 110, 112; Журавлев Д.А. Международный терроризм в информационно-коммуникативном пространстве мировой политики: дис. ... канд. политич. наук. М., 2011. С. 202.

безопасности, высокой финансовой и технологической оснащенностью не просто пользуются всеобъемлющим влиянием СМИ на потенциально огромную аудиторию, а создают собственные СМИ, радиочастоты, телевидение, выпускают книги, газеты, журналы и т.п. (в чем проявляется *непосредственный характер воздействия*).

Так, террористическая организация «Хезболла» (которая даже принимала участие в выборах в ливанский парламент) по данным некоторых СМИ имеет свои госпитали и больницы, школы и детские дома, где услуги медицины и образования гораздо дешевле, чем в государственных. «Хезболла» контролирует телеканал «Аль-Манар»²⁵⁸, радиостанцию «Аль-Нур», имеет свои печатные СМИ и веб-сайты²⁵⁹.

Палестинское исламистское движение «ХАМАС», признанное многими странами террористической организацией, имеет свою телестанцию «Хамас аль Акса».

В 2001 году Грузией была обнаружена радиостанция террористов «Станция свободной независимой Ичкерии – Кавказ», которая оказывала поддержку боевикам²⁶⁰.

Помимо этого, террористическими группами (организациями и сообществами) активно используется сеть Интернет для пропаганды, дезинформации, публичных призывов и оправдания терроризма, а также вовлечения в террористическую деятельность²⁶¹.

В октябре 2015 г. первый заместитель руководителя аппарата национального антитеррористического комитета Е.П. Ильин сообщил, что более 2700 российских граждан уехали под влиянием ИГИЛ воевать в

²⁵⁸ В 1990-е гг. Хезболла направляла вместе с каждой группой боевиков съемочные бригады, чтобы обеспечить свой телевизионный канал «Аль-Манар» требуемыми видеоматериалами. См.: Журавлев Д.А. Указ. соч. С. 123.

²⁵⁹ См.: Движение «Хезболлах» [Электронный ресурс]. URL: <http://ria.ru/spravka/20130610/942487146.html> (дата обращения: 11.05.2016).

²⁶⁰ См.: Чеченские боевики вещают на Россию из Грузии [Электронный ресурс]. URL: <http://www.rbc.ru/politics/19/07/2001/39934.shtml> (дата обращения: 14.06.2015).

²⁶¹ Американскими исследователями, проводившими мониторинг сети Интернет, были обнаружены пугающие данные о высокотехнологической вербовке со стороны Аль-Каиды. См.: Сапожонкова А.А. Интернет как инструментальное средство терроризма // Международный научно-исследовательский журнал. 2014. № 12-2 (31). С. 62.

Сирию²⁶². По другим данным таких людей почти в два раза больше – около 5000 человек²⁶³. Возрастающая роль информационно-психологического воздействия терроризма отмечается многими исследователями, которые подчеркивают необходимость тесного сотрудничества правоохранительных органов с психологами в разработке мер противодействия данному явлению²⁶⁴.

Безусловно, из названных и анализируемых способов использования информационно-психологического воздействия особую общественную опасность представляет непосредственное воздействие, и именно оно должно стать основой формирования понятия информационно-психологического терроризма.

Исходя из вышеизложенного и принимая во внимания существующие научные исследования по вопросам использования психологического воздействия, выделим следующие отличительные признаки информационно-психологического терроризма:²⁶⁵

- средством информационного воздействия выступает информация;
- тактическим объектом такого воздействия являются сознательно-волевые компоненты личности (социальной группы либо представителей власти), определяющие его (их) политические взгляды, поведение, настроения (в отношении, например, какой-либо иной социальной группы, политического деятеля, политического направления, избранного государством, и т.п.)²⁶⁶.

²⁶² См.: Выступление первого заместителя руководителя аппарата НАК Е.П. Ильина на Всероссийском семинаре-совещании руководителей патриотических объединений, 27.10.2015 [Электронный ресурс]. URL: <http://nac.gov.ru/publikacii/vystupleniya-i-intervyu/vystuplenie-pervogo-zamestitelya.html> (дата обращения: 06.11.2015).

²⁶³ См.: Эксперты оценили число воюющих за «ИГ» россиян в 5 тысяч человек, 17.06.2015 [Электронный ресурс]. URL: <http://www.interfax.ru/russia/447922> (дата обращения: 08.08.2015).

²⁶⁴ См.: Матчанова З.Ш. Указ. соч. С. 15.

²⁶⁵ См.: Сидоров П.И. Психический терроризм как форма несмертоносного оружия // Экология человека. 2005. № 7. С. 16; Глотина И.М. Указ. соч. С. 134; Кулибаба А.Н. Указ. соч. [Электронный ресурс]. URL: <http://law.edu.ru/doc/document.asp?docID=1252544> (дата обращения: 11.04.2016).

²⁶⁶ Наравне с названными признаками, информационно-психологическому терроризму присущи и другие, характерные для любого вида (формы) терроризма. См.: подробнее Глава 1 §1.

Таким образом, информационно-психологический терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах информационного пространства путем совершения действий, связанных с использованием информации и оказанием влияния на сознательно-волевые компоненты личности (социальной группы либо представителя власти).

На сегодняшний день к возможным угрозам информационно-психологического терроризма следует относить:

1) создание или размещение на уже существующих (в том числе не созданных террористическими группами (организациями или сообществами)) веб-сайтах информации, направленной на распространение пропаганды или дезинформации, публичных призывов, на публичное оправдание терроризма, а также на вовлечение физических и (или) юридических лиц (например, для финансирования терроризма) в террористическую деятельность;

2) создание и (или) руководство СМИ в целях распространения пропаганды, дезинформации, осуществления публичных призывов или оправдания терроризма, а также вовлечения физических и (или) юридических лиц в террористическую деятельность;

3) распространение информации иным способом (таким как листовки, объявления, брошюры, при непосредственном личном контакте и т.п.) в целях пропаганды, дезинформации, устрашения, публичных призывов, оправдания терроризма, а также вовлечения физических и (или) юридических лиц в террористическую деятельность.

4) иное информационно-психологическое воздействие, осуществляемое террористическими группами (организациями или сообществами) в информационном пространстве.

Информационно-технологический терроризм (кибертерроризм).

Данный вид информационного терроризма в международно-правовых документах и в законодательстве зарубежных стран получил название кибертерроризма²⁶⁷. Еще в 1930 г. на III Международной конференции по унификации уголовного законодательства в Брюсселе к возможным угрозам информационно-технологического терроризма были отнесены следующие действия: «самовольный перерыв нормальной работы транспорта, средств сообщений, железных дорог, телеграфа, телефона, почты, умышленную порчу гидравлического оборудования, освещения, отопления или двигательной силы общественного пользования или назначения»²⁶⁸. Так, один из обнаруженных компьютеров Аль-Каиды содержал информацию о проектировочных и структурных особенностях дамбы, полученных в сети Интернет и позволяющих инженерам данной террористической организации моделировать последствия атаки²⁶⁹.

На сегодняшний день общественная опасность информационно-технологического терроризма подчеркивается не только зарубежными исследователями. Российская государственная программа «Информационное общество» предусматривает в качестве одного из приоритетных направлений «противодействие использованию потенциала информационных технологий в целях предотвращения угрозы национальным интересам России»²⁷⁰.

Характеризуясь наличием присущих любому виду и формы терроризма признаков, общественная опасность информационно-технологического терроризма повышается за счет отдаленности преступников от места совершения террористического акта и других преступлений

²⁶⁷ См.: Касенова М.Б. Указ соч. [Электронный ресурс]. URL: <http://www.center-bereg.ru/h31.html> (дата обращения: 18.06.2015).

²⁶⁸ См.: Емельянов В.П. Терроризм и преступления с признаками терроризирования. СПб.: Изд-во Юридический центр Пресс, 2002. С. 19.

²⁶⁹ См.: Как современные террористы используют Интернет [Электронный ресурс]. URL: <http://www.alphagroup.kz/ru/media-files/stati/39-kak-sovremennye-terroristy-ispolzujut-internet> (дата обращения: 07.05.2016).

²⁷⁰ См.: Постановление Правительства Российской Федерации от 15.04.2014 № 313 (с изм. и доп. от 17.06.2015, № 602-ФЗ) «Об утверждении государственной программы Российской Федерации "Информационное общество (2011–2020)"» // СЗ РФ. 2014. № 18 (часть II), ст. 2159; 2015. № 26, ст. 3896.

террористической направленности²⁷¹. Этот факт стал определяющим для многих стран и всего международного сообщества в формировании специализированного понятийного аппарата и законодательства в сфере противодействия возможным угрозам в киберпространстве, в частности – угрозам кибертерроризма.

После событий, произошедших в 2001 г., Конгрессом США был принят новый правовой документ «Патриотический акт 2001 года», где появилось ранее неизвестное американскому законодательству понятие «кибертерроризм». К последнему же были отнесены различные квалифицированные формы хакерства и нанесения ущерба защищенным компьютерным сетям граждан, юридических лиц и государственных ведомств, включая ущерб, причиненный компьютерной системе, используемой государственным учреждением при организации национальной обороны или обеспечении национальной безопасности²⁷². Позднее вопросы противодействия угрозам в киберпространстве стали все больше интересовать мировое сообщество.

Очевидным недостатком понятия, предложенного американским законодательством, было сведение его к перечислению общественно опасных деяний, так или иначе признаваемых кибертерроризмом. Как видится, для создания данного понятия следует в первую очередь выделить его сущностные признаки.

На уровне доктрины российскими и украинскими учеными уже предпринимались попытки разработки понятия кибертерроризма на основе выделения его существенных признаков. В частности, Е.Н. Молодчая выделяла такие, как: общественная опасность; публичность; умышленное создание обстановки напряженности, страха; опосредованный характер воздействия; отдаленность от места непосредственного террористического

²⁷¹ См.: Белоножкин В.И., Остапенко Г.А. Указ. соч. С. 11.

²⁷² См.: Роговский Е.А. Указ. соч. [Электронный ресурс]. URL: <http://www.rusus.ru/?act=read&id=66> (дата обращения: 06.11.2015).

акта²⁷³. Однако при анализе указанных признаков прослеживается смешение автором понятий кибертерроризма и кибертеррористического акта, что, на наш взгляд, недопустимо.

Содержание понятия кибертерроризма, предложенного В.А. Голубевым, сводится к указанию его следующих признаков: объектом атаки выступает информация, обрабатываемая компьютером, компьютерная система и сети; атака сопряжена с опасностью гибели людей, причинения вреда здоровью или другими тяжкими последствиями; цель атаки – нарушение общественной безопасности, запугивание населения, провакация военного конфликта²⁷⁴. Очевидным достоинством выделяемых признаков является указание на объект атаки²⁷⁵, который, безусловно, отличается от других видов и форм терроризма. Однако видится чрезмерным выделение признака «создание опасности гибели людей, причинения вреда здоровью или других тяжких последствий», поскольку он в большей степени свойственен конкретным преступлениям, в частности – террористическому акту, нежели терроризму как явлению. Кроме того, согласно содержанию понятия терроризма, предложенного диссертантом, цель не является сущностным признаком терроризма, что относится непосредственно и к различным его видам и формам.

Анализ понятия кибертерроризма, предложенного Е.В. Старостиной, позволяет выделить следующие отличительные признаки: объектом атаки является охраняемая законом информация в критических сегментах государства, а также частном секторе, представленная в электронном виде на машинных носителях; средством атаки выступает информационная

²⁷³ См.: Молодчая Е.Н. Политика противодействия кибертерроризму в современной России: политологический аспект: дис. ... канд. политич. наук. М., 2011. С. 53-54.

²⁷⁴ См.: Голубев В.А. Кибертерроризм – миф или реальность // Центр исследования проблем компьютерной преступности [Электронный ресурс]. URL: <http://www.crime-research.org/library/terror3.htm> (дата обращения: 14.05.2016).

²⁷⁵ Представляется неудачным использование понятия «атака» для определения сущности кибертерроризма, поскольку оно приводит к очевидному смешению данного вида терроризма с кибертеррористическим актом. Данное утверждение относится и к понятию, предлагаемому Е.В. Старостиной, исследованному ниже по тексту диссертации.

система²⁷⁶. Соглашаясь с Е.В. Старостиной, полагаем, что отличительными признаками кибертерроризма являются объект, а именно тактический объект воздействия, и средства такого воздействия.

Тактическим объектом воздействия в кибертерроризме являются отдельные компоненты информационной среды и (или) инфраструктуры государств (к таковым следует относить как информационные системы государственных и частных организаций, так и критически важных объектов инфраструктуры государств (в том числе и объекты информационно-коммуникационной инфраструктуры)) либо организаций²⁷⁷. Средством информационно-технологического воздействия выступают информационные технологии и цифровые информационные ресурсы. Кроме того, информационно-технологическое воздействие может осуществляться только в пределах киберпространства, являющегося частью информационного пространства²⁷⁸.

Таким образом, информационно-технологический терроризм – *это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия)*

²⁷⁶ Помимо названных Е.В. Старостина выделяет и иные признаки, не являющиеся отличительными для данного вида терроризма. См.: Старостина Е.В. Проблема выработки единого понятия «кибертерроризм» и состав правонарушения в Российском законодательстве // Научная сессия МИФИ. 2006. Том. 14. С. 111-113.

²⁷⁷ Критически важные объекты инфраструктуры – объекты, системы, службы и институты, разрушение или выведение из строя которых может нанести серьезный ущерб социальному, экономическому или политическому порядку или национальной безопасности; объект информационно-коммуникационной инфраструктуры – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения функционирования такого объекта, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, а также персонала, который осуществляет их эксплуатацию; критический элемент критически важного объекта информационно-коммуникационной инфраструктуры – структурный компонент критически важного объекта информационно-коммуникационной инфраструктуры, выход из строя которого с неизбежностью приводит к нарушению или прекращению функционирования объекта в целом. См.: Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры», принятый Межпарламентской Ассамблеей государств-участников Содружества Независимых Государств. Приложение к Постановлению МПА СНГ от 28.11.2014 № 41-14 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

В законодательстве РФ под критически важным объектом понимается объект, нарушение или прекращение функционирования которого приведет к потере управления экономикой РФ, субъекта РФ или административно-территориальной единицы субъекта РФ, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения. См.: Федеральный закон от 21.12.1994 №68-ФЗ (с изм. и доп. от 23.06.2016, № 218-ФЗ) «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» // СЗ РФ. 1994. № 35, ст. 3648; 2016. № 26(ч.1), ст. 3887.

²⁷⁸ См.: подробнее Глава 2 §1.

органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах киберпространства, связанная с совершением противоправных действий в отношении отдельных компонентов информационной среды и (или) инфраструктуры государств либо организаций с помощью информационных технологий и (или) цифровых информационных ресурсов.

На сегодняшний день к возможным угрозам информационно-технологического терроризма следует относить совершение террористических актов с помощью информационных технологий в отношении отдельных элементов информационной среды и (или) инфраструктуры государств. Такие террористические акты характеризуются определенной спецификой. К возможным атакам на информационные системы по мнению В.А. Голубева следует относить: использование различных вредоносных компьютерных программ (компьютерных вирусов); использование средств подавления информационного обмена в сетях и организацию DDoS атак («отказ от обслуживания»); иные атаки, позволяющие проникнуть в информационную сеть или перехватить управление сетью²⁷⁹;

Кроме того, следует упомянуть о других общественно опасных деяниях, характеризующих террористическую деятельность в киберпространстве:

1) сбор с помощью различных технических устройств, обеспечивающих доступ к сети Интернет или иной локальной или территориальной сети, информации об объектах, о предметах, людях,

²⁷⁹ См.: Голубев В.А. Кибертерроризм – понятие, терминология, противодействие [Электронный ресурс]. URL: [http://sartracc.ru/i.php?oper=read_file&filename=Pub/golubev\(17-03-05\).htm](http://sartracc.ru/i.php?oper=read_file&filename=Pub/golubev(17-03-05).htm) (дата обращения: 06.05.2016).

мероприятиях, сооружениях и т.п., в том числе сведений, составляющих государственную, банковскую, коммерческую и иные виды тайн²⁸⁰.

2) руководство деятельностью террористической организации (сообщества), размещение стратегической и тактической информации о деятельности такой организации²⁸¹;

3) финансирование терроризма²⁸². Объемы финансовых потребностей террористических организаций зависят, в первую очередь, от размера такой организации. Сложноструктурированные террористические организации с органами управления требуют большего финансового обеспечения. На сегодняшний день финансовые средства необходимы террористическим организациям для совершения терактов, организации деятельности, обучения и т.п. Как отмечают эксперты, привлечение денежных средств очень часто осуществляется через благотворительные и коммерческие организации, в том числе находящиеся на базе сети Интернет²⁸³;

4) использование возможностей электронной почты, приложений Telegram, What's up и Viber для связи членов террористической организации (сообщества);

5) иное использование киберпространства для осуществления террористической деятельности.

Такие российские исследователи, как Е.А. Роговский, Е.Н. Молодчая, Т.Л. Тропина²⁸⁴, раскрывая сущность кибертерроризма, относят к последнему также информационно-психологическое воздействие на сознательно-волевые компоненты личности, социальной группы и т.д. Однако, по мнению автора

²⁸⁰ См.: Использование интернета в террористических целях // Управление Организации Объединенных Наций по наркотикам и преступности. Нью-Йорк, 2013. С. 10 [Электронный ресурс]. URL: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_inter_net_for_terrorist_purposes_Russian.pdf (дата обращения: 20.05.2016).

²⁸¹ См.: Там же. С. 8.

²⁸² См.: Там же. С. 7.

²⁸³ См.: Новые риски финансирования терроризма // Группа разработки финансовых мер борьбы с отмыванием денег. 2015. С. 23 [Электронный ресурс]. URL: http://www.cbr.ru/today/anti_legalisation/fatf/Emerging-Terrorist-Financing-Risks_Russian.pdf (дата обращения: 17.05.2016).

²⁸⁴ См.: Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. Владивосток, 2005. С. 69.

данного диссертационного исследования, не следует ограничивать информационно-психологическое воздействие лишь сферой киберпространства (то есть сетью Интернет, иной локальной сетью). Для информационно-психологического воздействия характерно также использование классических СМИ (газет, журналов), а также телевидения, радио, иных средств коммуникации (таких как листовки, объявления и т.п.), а равно непосредственного личного общения (вовлечения, пропаганды) с лицом, на которое оказывается воздействие.

В настоящее время общественная опасность именно информационно-психологического воздействия террористических групп (организаций или сообществ) возросла в связи с активным вовлечением населения, в частности Российской Федерации, в террористические организации по типу ИГИЛ²⁸⁵.

Исходя из вышеизложенного информационно-психологический терроризм и информационно-технологический терроризм различаются по средствам воздействия и тактическим объектам воздействия. Каждый из названных видов информационного терроризма характеризуется повышенной общественной опасностью, что обусловлено расширением сферы информационного пространства, ее доступностью и низкой правовой защищенностью. В этой связи существует необходимость в совершенствовании и разработке новых мер уголовно-правового и иного характера в противодействии информационному терроризму.

²⁸⁵ См.: Владимир Путин обеспокоен вовлечением в ИГИЛ граждан России [Электронный ресурс]. URL: <http://www.pravmir.ru/vladimir-putin-obespokoen-vovlecheniem-v-igil-grazhdan-rossii/> (дата обращения 06.11.2015).

ГЛАВА 3. УГОЛОВНО-ПРАВОВЫЕ И ИНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ

§1. Уголовно-правовые меры противодействия информационному терроризму

Уголовно-правовая политика в сфере противодействия терроризму реализуется в том числе посредством установления уголовной ответственности за преступления террористической направленности²⁸⁶. Задачами уголовного законодательства на сегодняшний день являются охрана наиболее важных общественных отношений, круг которых определен в статье 2 УК РФ, а также предупреждение совершения преступлений. Законодательное конструирование состава и определение вида и размера наказания, соответствующего общественной опасности противоправного деяния, способствуют реализации указанных задач. На протяжении существования норм об ответственности за преступления террористической направленности прослеживается тенденция усиления наказания за данные деяния, а также увеличения количества их составов²⁸⁷.

Нестабильность внутренней экономики, сложная внешнеполитическая ситуация, а также продолжающийся процесс социального регресса, обусловленного падением нравственности, объективно отразились на состоянии преступности²⁸⁸. В условиях глобализации информационного пространства возросло влияние информации на сознательно-волевые компоненты личности, а развитие в сфере информационных технологий способствовало возникновению новых угроз. С учетом этого уголовное

²⁸⁶ См.: Макеева Н.В. Приоритеты уголовной политики Российской Федерации на современном этапе // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2012. № 3 (23). С. 6.

²⁸⁷ Последние изменения в УК РФ, внесенные Федеральным законом от 06.07.2016 № 375-ФЗ, связаны, в том числе, с увеличением низшего предела санкции по ч. 1 ст. 205 УК РФ с восьми до десяти лет.

²⁸⁸ За 2015 год было зарегистрировано 2352,1 тыс. преступлений, что на 8,6% больше, чем за 2014 год. Из них 1531 преступление террористической направленности, что на 35,8% больше, чем в 2014 году. См.: Состояние преступности – январь-декабрь 2015 года [Электронный ресурс]. URL: <https://mvd.ru/folder/101762/item/7087734/> (дата обращения: 18.05.2016).

законодательство должно адекватно реагировать на происходящие изменения.

Поскольку информационный терроризм подразделяется на информационно-технологический и информационно-психологический, целесообразным, на наш взгляд, будет систематизировать уголовно-правовые меры противодействия информационному терроризму в зависимости от выделяемых видов.

Уголовно-правовые меры противодействия информационно-технологическому терроризму (кибертерроризму).

Кибертерроризм как явление, возникшее в пределах киберпространства, вызывает серьезные опасения у российских и зарубежных ученых²⁸⁹. В особенности это касается кибертеррористических актов (киберактов). Законодательство Англии и США является одним из примеров оперативного реагирования на возрастающую угрозу совершения террористических актов в киберпространстве. Так, в Англии к террористическим актам отнесены также действия, связанные с выведением из строя компьютеров, нарушением снабжения электричеством и водой²⁹⁰. Закон США «О борьбе с терроризмом» 2001 г. определяет в качестве киберактов квалифицированные формы хакерства и нанесения ущерба защищенным компьютерным сетям граждан, организаций (юридических лиц) и государственных ведомств, которые могут повлечь в том числе, причинение физического вреда и т.п.²⁹¹.

²⁸⁹ См.: Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУРа. 2010. № 1. С. 41; Голубев В.А., Сайтарлы Т.А. Проблемы борьбы с кибертерроризмом в современных условиях // Центр исследования проблем компьютерной преступности [Электронный ресурс]. URL: <http://www.crime-research.org/library/e-terrorism.htm> (дата обращения: 18.05.2016). Частные вопросы киберпреступности и кибертерроризма были рассмотрены в работах Т.Л. Тропиной, Е.Н. Молодчей, а также Центром исследования компьютерных преступлений под руководством В.А. Голубева. См.: Тропина Т.Л. Указ. соч. С. 12; Молодчая Е.Н. Указ. соч. С. 17; Computer Crime Research Center [Электронный ресурс]. URL: <http://www.crime-research.org/feedback/> (дата обращения: 18.05.2016).

²⁹⁰ См.: Уголовное право зарубежных стран. Общая и Особенная части: учебник для магистров / Н.А. Голованова, Е.В. Еремин, М.А. Игнатова [и др.]; под ред. Н.Е. Крыловой. 4-е изд., перераб. и доп. М.: Изд-во Юрайт, 2013. С. 645.

²⁹¹ См.: Там же. С. 771-772.

На сегодняшний день в условиях информационной глобализации угроза совершения кибертеррористического акта вполне реальна. Согласно данным, полученным в ходе опроса населения, подавляющее число респондентов определяют вероятность совершения информационно-технологического террористического акта как высокую²⁹².

Однако, прежде чем говорить о необходимости внесения изменений в УК РФ, связанных с установлением уголовной ответственности за совершение кибертеррористического акта, следует проанализировать некоторые положения действующего законодательства.

Так, адекватных изменений, в том числе с учетом уже разработанных положений данного диссертационного исследования, требует ст. 205 УК РФ, устанавливающая ответственность за террористический акт, в части уточнения некоторых объективных и субъективных признаков основного состава. На его несовершенство уже не раз указывали такие авторы, как Н.А. Лопашенко²⁹³, В.Е. Петрищев²⁹⁴, М.Ф. Мусаелян²⁹⁵, В.П. Емельянов²⁹⁶ и др.

Общественная опасность любого преступления определяется главным образом ценностью объекта, на который оно посягает²⁹⁷. Родовым объектом преступления, предусмотренного ст. 205 УК РФ, выступает общественная безопасность и общественный порядок, что обуславливается нахождением данного состава в соответствующем разделе УК РФ (раздел IX УК РФ), видовым – общественная безопасность (глава 24 УК РФ). Кроме того, его непосредственным основным объектом также выступает общественная безопасность.

²⁹² См.: Прил. № 6. С. 268.

²⁹³ См.: Лопашенко Н.А. Уголовная политика. М.: Волтерс Клувер, 2009. С. 372-375.

²⁹⁴ См.: Петрищев В.Е. Защита объектов террористических посягательств и проблемы информационного противоборства // Организованный терроризм и организованная преступность / под ред. А.И. Долговой. М.: Российская криминологическая ассоциация, 2002. С. 33-34.

²⁹⁵ См.: Мусаелян М.Ф. Террористический акт: уголовно-правовой аспект: дис. ... канд. юрид. наук. М., 2007. С. 11

²⁹⁶ См.: Емельянов В.П. Терроризм и преступления с признаками терроризирования: уголовно-правовое исследование. СПб.: изд-во Юридический центр Пресс, 2002. С. 189.

²⁹⁷ См.: Карпушин М.П. Курляндский В.И. Уголовная ответственность и состав преступления. М.: Юрид. лит., 1974. С. 167-168.

Категория общественной безопасности весьма сложная. На сегодняшний день в литературе сформировалось множество точек зрения о сущности и содержании данного понятия. Общественная безопасность определяется как в узком, так и в широком смысле этого слова, что объясняется различными подходами к пониманию объекта преступления (как блага или как общественного отношения), отсутствием законодательного закрепления понятия общественной безопасности, а также его использованием для раскрытия сущности общего, родового, видового и непосредственного объектов определенной группы преступлений.

Следует сказать, что отсутствие законодательной регламентации понятия общественной безопасности предопределяет проблемы, связанные с обеспечением уголовно-правовой охраны, а также трудностью в квалификации и разграничении смежных составов преступлений. С появлением новых видов и форм терроризма более остро встал вопрос о квалификации по ст. 205 УК РФ возможных террористических актов посредством иных, не менее общественно опасных действий, на иной платформе. В первую очередь эти проблемы связаны с определением объекта преступления.

На сегодняшний день на законодательном уровне лишь определено место общественной безопасности как вида национальной безопасности наравне с безопасностью государства, экологической безопасностью, безопасностью личности (законодатель предлагает неисчерпывающий перечень)²⁹⁸ и т.д.

Выделение общественной безопасности как отдельного вида, отличного от экологической или, например, информационной, достаточно спорно. Это связано с тем, что посягательства на экологическую безопасность довольно часто сопровождаются негативными изменениями в общественных отношениях, складывающихся по поводу обеспечения

²⁹⁸ См.: Федеральный закон от 28.12.2010 № 390-ФЗ (с изм. и доп. от 05.10.2015, № 285-ФЗ) «О безопасности» // СЗ РФ. 2011. № 1, ст. 2; 2015. № 41 (ч. II), ст. 5639.

общественной безопасности или даже безопасности государства (в зависимости от масштаба экологического бедствия).

Об относительной условности разделения национальной безопасности на безопасность личности, общества и государства также указывала И.Б. Кардашова. Если представить, что личность – это индивид, характеризующийся устойчивой системой социальных связей²⁹⁹, а общество (в самом широком смысле этого слова) – совокупность индивидов³⁰⁰, личная безопасность в некотором смысле зависит от безопасности общества в целом³⁰¹. Таким образом, определяется очень тонкая грань в выделении видов безопасности, а на уровне уголовно-правовой охраны следует говорить лишь о приоритете одного вида безопасности над другим, обусловленном выделением основного, дополнительного или факультативного объектов преступления.

Ученые справедливо отмечают необходимость исследования данного понятия, исходя из сущности его исходных³⁰². К таковым в первую очередь относят понятие «безопасность». Чаще всего в научной литературе³⁰³ и словарях³⁰⁴ оно раскрывается как состояние защищенности. При этом под защищенностью следует понимать способность сохранения объектами или системой (такой как природа, человек, общество, государство и др.) своей

²⁹⁹ См.: Философия: учебник для вузов / В.В. Васильев, П.П. Гайденок, А.Ф. Зотов [и др.]; под общ. ред. В.В. Миронова. М.: Норма, 2005. С. 647.

³⁰⁰ См.: Черданцев А.Ф. Теория государства и права: учебник для вузов. М.: Юрайт, 2002. С. 70.

³⁰¹ См.: Кардашова И.Б. Укрепление конституционных основ общественной безопасности // Законы России: опыт, анализ, практика. 2010. № 4. С. 111.

³⁰² См.: Жаглин А.В. Общественная безопасность как социальное явление и элемент системы национальной безопасности // Вестник Воронежского института МВД России. 2007. № 1. С. 32; Нестеров С.В. Понятие общественной безопасности // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2013. № 11 (127). С. 3; Арзамасцев Н.И. Административно-правовое обеспечение органами внутренних дел общественной безопасности при чрезвычайных ситуациях техногенного характера: дис. ... канд. юрид. наук. М., 2002. С. 11.

³⁰³ См.: Курс уголовного права. Особенная часть / под ред. Г.И. Борзенкова, В.С. Комиссарова. Т. 4. М.: Зерцало, 2002. С. 173; Тихий В.П. Уголовная ответственность за нарушение правил безопасности обращения с общепасными предметами. Киев: Изд-во УМК ВО при Минвузе УССР, 1989. С. 6; Рыбалкин Н.Н. Природа безопасности: автореф. дис. ... д-ра философ. наук. М., 2003. С. 14.

³⁰⁴ См.: Ожегов С.И. Шведова Н.Ю. Указ. соч. С. 41.

качественной определенности и возможности выполнения своих функций и задач в условиях воздействия негативных факторов³⁰⁵.

Другим исходным понятием общественной безопасности является «общество». В теории государства и права общество определяется как сложная, динамическая система, сущность которой проявляется в различного рода отношениях, возникающих между индивидами и их объединениями, удовлетворяющими свои потребности за счет поддержания целостного и прогрессивного саморазвития социального объединения³⁰⁶. Другими словами, общественную безопасность следует понимать как состояние защищенности различного рода общественных отношений, возникающих между индивидами и их объединениями.

Некоторые исследователи раскрывают понятие общественной безопасности через состояние защищенности личности, общественного спокойствия³⁰⁷. Другие связывают общественную безопасность также с нормальной координацией общественной жизни государством³⁰⁸. Это обусловлено тем, что общество исторически опережает возникновение государства, определяя место последнего как часть политической сферы жизни общества. Однако такой подход ряд авторов определяют как расширительный, приводящий к смешению с объектами преступлений против личности и против государственной власти³⁰⁹.

Само по себе общество представляется абстрактной категорией как система, содержательную сторону которой составляют различного рода

³⁰⁵ См.: Общая теория национальной безопасности: учебник / под общ. ред. А.А. Прохожева. М.: Изд-во РАГС, 2005. С. 13.

³⁰⁶ См.: Кулапов В.Л. Теория государства и права: электронный учебник. Саратов: Изд-во ФГБОУ ВПО «СГЮА», 2011 [Электронный ресурс]. URL: <http://smolsgua.ru/wp-content/uploads/2014/02/Теория-государства-и-права.pdf> (дата обращения: 28.05.2016).

³⁰⁷ См.: Кондрашов Б.П. Общественная безопасность и административно-правовые средства ее обеспечения. М.: Щит-М, 1998. С. 8.

³⁰⁸ См.: Кондрашов Б.П. Указ. соч. С. 8; Курс уголовного права. Особенная часть / под ред. Г.И. Борзенкова, В.С. Комиссарова. Т. 4. М.: Зерцало, 2002. С. 173.

³⁰⁹ См.: Герасимов А.П. Роль государства и права в обеспечении социальной безопасности // Общая теория права и государства: учебник / под ред. В.В. Лазарева. 3-е изд., перераб. и доп. М.: Юрист, 2001. С. 471-472; Цит. по: Закомолдин Р.В. О трюйственности понятия «общественная безопасность» в нормах действующего УК РФ [Электронный ресурс]. URL: http://nutego.ucoz.com/index/o_trojstvennosti_ponjatija_quot_obshestvennaja_bezopasnost_quot/0-69#_ftn8 (дата обращения: 18.05.2016).

общественные отношения, складывающиеся между индивидами (их объединениями), организациями, институтами. Отличие исследуемого объекта уголовно-правовой охраны следует проводить по следующему критерию: совершение преступления, относящегося к группе преступлений против общественной безопасности, потенциально создает угрозу для нормальной жизнедеятельности неопределенного круга людей, то есть для нормального протекания важных и значимых общественных процессов³¹⁰.

В связи с вышеизложенным общественную безопасность следует понимать как *состояние защищенности, обеспечивающее безопасное существование общественных отношений, складывающихся между индивидами и их объединениями, а также нормальную (регламентированную правовыми актами, в том числе внутриведомственными) координацию общественной жизни государством*³¹¹.

Такое содержание понятия общественной безопасности направлено на защиту важнейших компонентов общественной жизни: прав и законных интересов отдельных индивидов, общественных объединений и организаций, а также нормальной деятельности государства, выступающего частью политической сферы жизни общества.

Итак, основным непосредственным объектом преступления ст. 205 УК РФ выступает общественная безопасность.

Объективная сторона как один из элементов состава преступления занимает немаловажное место в квалификации террористического акта. Обязательным признаком объективной стороны исследуемого состава (как и любого другого) выступает деяние. На сегодняшний день существует две точки зрения на вопрос понимания сущности основных признаков объективной стороны террористического акта. Подавляющее большинство

³¹⁰ См.: Зеркалов Д.В. Общественная безопасность. Киев: Основа, 2012 [Электронный ресурс]. URL: <http://zerkalov.kiev.ua/sites/default/files/ob-m.pdf> (дата обращения: 28.05.2016).

³¹¹ В качестве субъектов отношений общественной безопасности следует определять государство, органы, его представляющие, группы людей, коллективы, отдельных граждан. См.: Гурбанов А.Г., Павлик М.Ю., Михайлов Н.Н. Общественная безопасность как объект уголовно-правовой охраны // Вестник Санкт-Петербургского университета МВД России. 2006. № 1. С. 171.

ученых склоняются (вполне обоснованно) к тому, что деяние, предусмотренное ч. 1 ст. 205 УК РФ (основной состав), выражается в совершении взрыва, поджога и иных действий³¹². Согласно другой точке зрения взрыв, поджог и иные действия – это способы совершения террористического акта³¹³. В последнем случае автор проводит аналогию с составами, предусмотренными ч. 2 ст. 167, ч. 3 ст. 261 УК РФ, где названные выше действия выступают в качестве способов совершения преступления.

Есть основания согласиться с пониманием взрыва, поджога и иных действий как деяний изучаемого состава, поскольку их определение как способов совершения преступления требовало бы иной законодательной конструкции (например, такой как: совершение общеопасных действий путем взрыва, поджога или иным способом).

Как следует из диспозиции ч. 1 ст. 205 УК РФ, перечень действий, отражающих суть деяния, не является исчерпывающим. К таковым, согласно положениям Постановления Пленума ВС РФ от 09.02.2012 № 12 следует также относить иные действия, сопоставимые по последствиям со взрывом или с поджогом, например: устройство аварий на объектах жизнеобеспечения, разрушение транспортных коммуникаций и т.п. Названные и подобные им действия согласно диспозиции ч. 1 ст. 205 УК РФ должны иметь устрашающий население характер и создавать опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий. В этой связи возникает вопрос о возможности признания отдаленных действий, связанных с использованием информационных технологий для отключения или изменения работы внутренних автоматизированных информационных систем, например электростанции, водохранилища, больницы, как деяний, сопоставимых по последствиям со взрывом или с поджогом.

³¹² См.: Бытко Ю.И., Бытко С.Ю. Уголовное право России: части Общая и Особенная / под ред. д-ра. юрид. наук, проф., заслуженного юриста РФ Ю.И. Бытко. Саратов: Научная книга, 2011. С. 168; Российское уголовное право. Курс лекций: в 3 т. Т. 3. Особенная часть (главы XI-XXI) / А.В. Наумов. 4-е изд., перераб. и доп. М.: Волтерс Клувер, 2008. С. 27.

³¹³ См.: Мусаелян М.Ф. Указ. соч. С. 84.

На сегодняшний день исследователи в области обеспечения безопасности констатируют факт возрастающей роли информационных технологий по сравнению с ядерным оружием, поскольку последнее ограничено в применении³¹⁴.

Кроме того, уже не редкость появление сведений о фактах взлома информационных систем крупнейших организаций, которым в результате был причинен многомиллионный ущерб. Одна из последних хакерских атак на компанию Sony способствовала получению злоумышленниками номеров банковских карт вместе с реквизитами владельцев³¹⁵. Безусловно, речь не идет в данном случае о кибертерроризме (информационно-технологическом терроризме), однако увеличение подобного рода деяний свидетельствует о возрастающей угрозе информационной безопасности.

В настоящее время многие зарубежные страны «вербуют» талантливых хакеров для использования навыков последних в обеспечении информационной безопасности государства³¹⁶. Так действуют и крупные террористические организации (сообщества), которые привлекают «суррогатные силы» в целях посягательства на информационную безопасность государств.

В 1985 году в Японии леворадикальная группировка с помощью компьютерных систем предприняла атаку на единую сеть управления железной дорогой³¹⁷. Несколько лет назад неизвестные совершили компьютерную атаку на высокозащищенный иранский ядерный центр с помощью вируса Stuxnet, которая поразила 1368 из 5000 центрифуг на заводе

³¹⁴ См.: Ермаков Сергей: ядерное оружие вытеснят информационные технологии [Электронный ресурс]. URL: http://www.pravda.ru/news/expert/15-12-2014/1240108-Sergey_Ermakov-0/ (дата обращения: 14.04.2016).

³¹⁵ См.: Sony Pictures официально прокомментировала взлом своих серверов хакерами // Новости высоких технологий [Электронный ресурс]. URL: <http://hi-news.ru/computers/sony-pictures-officialno-prokommentirovala-vzлом-svoix-serverov-xakerami.html> (дата обращения 16.05.2016).

³¹⁶ Корпус стражей исламской революции, являясь элитным иранским военно-политическим формированием, прибегает к помощи иранского сообщества хакеров для посягательств на государственные объекты. См.: Siavash «Iranian Cyber Warfare Threat Assessment» // Siavash's Blog [Электронный ресурс]. URL: <http://www.cyberwarzone.com/content/iranian-cyber-warfare-threat-assessment> (дата обращения: 27.04.2016).

³¹⁷ См.: Кибератака реальной войны [Электронный ресурс] URL: http://www.e-reading.club/chapter.php/75936/106/Kurushin_-_100_velikih_voennyh_taiin.html (дата обращения: 17.05.2016).

по обогащению урана, а также сорвала сроки запуска ядерной АЭС³¹⁸. Последнее событие стало первым фактом начавшегося масштабного использования киберпространства в преступных целях.

Проведенный опрос респондентов – граждан разного рода занятий (от студентов до профессоров и сотрудников правоохранительных органов) – показал, что они воспринимают возможные последствия в результате вмешательства в работу отдельных компонентов информационной среды как серьезные, связанные с возможностью гибели людей или причинения значительного экономического ущерба региону, вреда экологии и др.³¹⁹

На сегодняшний день ч. 1 ст. 205 УК РФ предполагает широкую трактовку общественно опасных деяний, позволяющую относить к террористическому акту посягательства с помощью информационных технологий на основные компоненты информационной среды и (или) инфраструктуры государств, если они устрашают население и создают опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий. При информационно-технологическом акте страх возникает в результате получивших общественный резонанс деяний³²⁰ и может быть усилен с помощью публичных заявлений террористов.

Объективная сторона исследуемого преступления может также выражаться в угрозе совершения указанных действий, причем такая угроза должна вызывать у граждан и органов власти обоснованное реальное опасение ее осуществления. Некоторые ученые ставят под сомнение такое приравнивание, полагая, что угроза менее общественно опасна, чем террористическое действие, в связи с чем следует предусмотреть привилегированный состав преступления, устанавливающий менее строгую

³¹⁸ См.: Бенитес Х., Хили Д. США. Воздушные замки кибербезопасности // Владивостокский центр исследования организованной преступности [Электронный ресурс]. URL: <http://topwar.ru/18781-vozdushnye-zamki-kiberbezopasnosti.html> (дата обращения: 28.05.2016).

³¹⁹ Прил. № 6. С. 268.

³²⁰ См.: Молодчая Е.Н. Указ. соч. С. 53-54.

уголовную ответственность, чем за совершение действий, указанных в диспозиции ч. 1 ст. 205 УК РФ³²¹.

С этим вряд ли можно согласиться, имея в виду общественную опасность данного преступления, обусловленную масштабностью подобных угроз и непредсказуемостью их отдаленных последствий. В связи с этим не следует выделять угрозу совершения действий, указанных в диспозиции ч. 1 ст. 205 УК РФ, в отдельный привилегированный состав. Наличие альтернативной относительно-определенной санкции в ч. 1 ст. 205 УК РФ позволяет индивидуализировать наказание в зависимости в том числе от фактических обстоятельств дела³²².

Некоторого переосмысления требуют признаки субъективной стороны преступления ч. 1 ст. 205 УК РФ. Являясь обязательным элементом любого состава преступления, субъективная сторона и входящие в нее признаки выступают (довольно часто) определяющим критерием разграничения смежных составов. Как внутренняя сторона преступления, субъективная сторона порождает, направляет и определяет характер действий, включенных в объективную сторону преступления³²³.

Обязательными признаками субъективной стороны основного состава, предусмотренного ст. 205 УК РФ, являются вина в форме прямого умысла и специальная цель.

Прежде (до мая 2014 года³²⁴) ч. 1 ст. 205 УК РФ предусматривала цель воздействия на принятие решения органами власти или международными организациями, что порождало некоторые проблемы в квалификации совершаемых террористических актов. Во-первых, среди объектов воздействия отсутствует указание на орган местного самоуправления, физическое лицо, социальную группу или юридическое лицо. Во-вторых,

³²¹ См.: Мусаелян М.Ф. Указ. соч. С. 98.

³²² На это обращает внимание и А.В. Бриллиантов. См.: Бриллиантов А.В. Уголовная ответственность за терроризм и захват заложников: лекция. М.: ИПК РК Ген. прокуратуры РФ, 2004. С. 15.

³²³ См.: Кудрявцев В.Н. Объективная сторона преступления. М.: Госюриздат, 1960. С. 12-13.

³²⁴ См.: Федеральный закон от 05.05.2014 № 130-ФЗ (с изм. и доп. от 03.07.2016, № 305-ФЗ) «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2014. № 19, ст. 2335; 2016. № 27 (ч. II), ст. 4238.

исходя из содержания диспозиции ч. 1 ст. 205 УК РФ, воздействие должно осуществляться на принятие решения органами власти, международными организациями – во множественном числе, что, на наш взгляд, не совсем верно. Все это стало основанием для внесения изменений в определение целей террористического акта. На сегодняшний день законодатель предусматривает ответственность за совершение указанных в диспозиции ч. 1 ст. 205 УК РФ действий с двумя альтернативными целями:

- воздействия на принятие решений органами власти или международными организациями;
- дестабилизации деятельности органов власти или международных организаций.

Воздействие на принятие решений органами власти или международными организациями как цель террористического акта не раз подвергали вполне обоснованной критике³²⁵. Соглашаясь с некоторыми авторами в необходимости расширения круга объектов, на которые осуществляется воздействие, поведенческих форм его адресатов, а также учитывая, кроме того, выводы, сделанные диссертантом³²⁶, предлагаем следующую редакцию исследуемой цели: *воздействие на принятие решения или совершения действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом.*

Вторая альтернативная цель террористического акта требует более тщательного и всестороннего исследования. Содержание понятия «дестабилизация» в буквальном смысле определяется как отсутствие стабильности. На сегодняшний день ни на уровне доктрины, ни на уровне законодательства не разъясняется содержание данного понятия. Однако в достаточной мере в диссертационных и иных научных исследованиях

³²⁵ См.: Галкин А.Б. Субъективные признаки состава террористического акта // Молодой ученый. 2014. № 12 [Электронный ресурс]. URL: <http://www.moluch.ru/archive/71/12264/> (дата обращения: 20.05.2016); Емельянов В.П. Понятие терроризма в уголовном законодательстве России и Украины. Сравнительный анализ // Российская юстиция. 1999. № 11. С. 42.

³²⁶ См.: Глава 1 §1.

раскрываются вопросы определения таких понятий, как социальная и политическая стабильность (нестабильность).

Категория стабильности довольно часто используется при характеристике политического, социального, экономического развития общества. Политическая стабильность как часть социальной стабильности представляет собой особую ценность для демократического правового государства, поскольку является гарантом высокого уровня легитимности власти при управлении социальными процессами, а равно соблюдения прав, свобод и законных интересов индивидов и их объединений³²⁷.

Политическая нестабильность – это состояние, характеризующееся приближением показателей развития всех основных подсистем (уровня легитимности власти и т.п.) к предельно-критическим величинам, обуславливающим состояние кризиса³²⁸.

Между тем понятие дестабилизации связывают с глагольной формой «дестабилизировать», то есть совершить действия, нарушающие стабильность чего-либо. Исследователями также отмечается, что дестабилизация характеризуется *такими изменениями в политической системе, которые не ожидалась и были нежелательными*³²⁹.

О политической и социальной дестабилизации в различных аспектах упоминается в исследованиях о противодействии терроризму. Так, она рассматривается в качестве фактора, способствующего увеличению террористических проявлений. Кризисные процессы, по мнению некоторых исследователей, сопровождаются усилением оппозиционных движений, в том числе и террористических³³⁰.

³²⁷ См.: Бабошин К.И. Социально-политическая стабильность в современной России: социологический анализ: дис. ... канд. философ. наук. Саратов, 2005. С. 13.

³²⁸ См.: Ярославцева А.О. Политическая стабильность и конфигурации политической элиты: интерпретативный потенциал и границы применимости теоретических подходов: дис. ... канд. политич. наук. М., 2012. С. 40.

³²⁹ См.: Там же. С. 41.

³³⁰ См.: Путилин Б.Г. Кризис и международный терроризм // Материалы Конференции в ИМЭМО РАН, 20-21 апреля 2009 «Глобальный кризис и проблемы обеспечения общественно-политической стабильности: опыт стран Запада и Россия» / ред. Н.В. Загладин. М., ИМЭМО РАН, 2009. С. 124

Другие авторы полагают, что терроризм выступает дестабилизирующим фактором современного общественно-политического развития. В числе дезорганизирующих признаков называют: преднамеренное создание обстановки напряженности, страха, порождение общей опасности и др.³³¹

Кроме того, существует мнение, что одной из альтернативных целей террористического акта может выступать дестабилизация политической или социальной обстановки³³².

Установление альтернативной цели террористического акта – дестабилизации деятельности органов власти или международных организаций – было направлено на решение ряда проблем в квалификации деяний по ст. 205 УК РФ³³³. Это обусловлено тем, что «воздействие» в правоприменительной практике характеризуется, чаще всего, предъявлением требований к представителям власти.

На сегодняшний день в действительности приходится констатировать тот факт, что некоторые террористические проявления подверглись изменениям: уровень финансирования, организации и сами террористические акты. Об этом свидетельствуют недавние события, произошедшие в Париже, которые также не сопровождались предъявлением каких-либо требований, либо же таковые подразумевались, но не высказывались органам власти или международным организациям³³⁴. Между тем непредъявление требований вовсе не означает отсутствие цели воздействия. Она проявляется в последующих действиях террористов, выраженных во взятии на себя

³³¹ См.: Ефанова Е.В. Терроризм как фактор политической дестабилизации современного российского общества: дис. ... канд. политич. наук. Волгоград, 2006. С. 11.

³³² При этом автором не разъясняется сущность предлагаемой цели. См.: Коновалова А.Б. Террористический акт в форме угрозы и заведомо ложное сообщение об акте терроризма как проявления информационного терроризирования: дис. ... канд. юрид. наук. Киров, 2008. С. 153-159.

³³³ Определенные сомнения, в частности, вызвала квалификация по ст. 205 УК РФ взрывов на железнодорожном вокзале, а также в троллейбусе (Волгоград, 2013 г.), что обусловлено непредъявлением каких-либо требований органам власти или международным организациям. Таким образом, по мнению ряда СМИ, отсутствовала цель террористического акта, являющаяся обязательным признаком субъективной стороны.

³³⁴ См.: Теракты в Париже – объявление войны [Электронный ресурс]. URL: <http://www.apn.ru/publications/article34327.htm> (дата обращения: 20.06.2016).

ответственности за совершенные террористические акты. Тем самым, террористические группы (организации, сообщества) демонстрируют свое влияние, силу и власть. Дестабилизация деятельности органа власти, органа местного самоуправления и т.д., в свою очередь, всегда объективно существует наравне с целью воздействия.

Однако анализ приговоров в части установления целей террористического акта и заведомо ложного сообщения об акте терроризма (ст. 207 УК РФ) свидетельствует о возникновении новой проблемы.

В соответствии с действующим законодательством преступление, предусмотренное ст. 207 УК РФ, не относится к преступлениям террористической направленности³³⁵. Однако в научной литературе не остается без внимания вопрос о разграничении угрозы совершения террористического акта и заведомо ложного сообщения об акте терроризма. В числе критериев разграничения называют:

1) субъект преступления (в ст. 205 УК РФ – это террористы; в ст. 207 УК РФ – лица, не являющиеся террористами, пособниками и другими, кто так или иначе связан с террористической деятельностью);

2) сущность деяний и характер угроз (сообщений), предусмотренных статьями 205 и 207 УК РФ, различны.

3) мотивы и цели действий, предусмотренных статьями 205 и 207 УК РФ, различны³³⁶. Данный критерий требует некоторого разъяснения. В первую очередь затруднения возникают при разграничении целей угрозы совершения действий, указанных в ч. 1 ст. 205 УК РФ, и заведомо ложного сообщения об акте терроризма. В соответствии с ч. 1 ст. 207 УК РФ цель не является обязательным признаком субъективной стороны данного состава, однако ее установление может учитываться при назначении наказания. Анализ 94 приговоров районных, городских, Верховных судов различных

³³⁵ См.: Указание Генпрокуратуры России № 65/11, МВД России № 1 от 01.02.2016 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

³³⁶ См.: Овчинникова Г.В. Терроризм: серия «Современные стандарты в уголовном праве и уголовном процессе» / науч. редактор проф. Б.В. Волженкин. СПб., 1998. С. 22-23.

регионов РФ (Саратовской, Самарской, Владимирской, Белгородской областей, Удмуртской, Чувашской республик и др.) за 2012 г. по июнь 2016 г. по уголовным делам о привлечении к уголовной ответственности за заведомо ложное сообщение об акте терроризма³³⁷ в части определения мотивов и целей данного преступного деяния показал следующее. Хулиганские побуждения послужили мотивом совершения преступления по ст. 207 УК РФ в 29% случаев. В 18% случаев целью совершения такого преступления явилась *дезорганизация деятельности органов и учреждений*. Личные мотивы привели к совершению данного преступления в 15% случаев. В 9% случаев данное преступление было совершено с целью наведения паники.

Предполагаем, что сущностное содержание дестабилизации и дезорганизации очень схожее, хоть и не совпадающее. Так, исследователи отмечают, что одним из факторов дестабилизации является дезорганизация, то есть нарушение установленного порядка³³⁸. Такое определение содержания целей террористического акта и заведомо ложного сообщения об акте терроризма может привести к признанию вновь ст. 207 УК РФ в качестве преступления террористической направленности, что нельзя признать верным. В связи с этим, п. 4 Постановления пленума ВС РФ от 09.02.2012 № 12 необходимо дополнить следующим: *«Действия, предусмотренные ст. 207 УК РФ, не могут совершаться с целью воздействия на принятие решения или совершения действия (бездействия) органом власти, органом местного самоуправления, международной организации, социальной группой, юридическим лицом или физическим лицом и с целью дестабилизации деятельности органа власти, органа местного самоуправления или международной организации»*.

³³⁷ См.: Прил. № 2. С. 240; Прил. № 3. С. 247.

³³⁸ См.: Ахиезер А.С. Дезорганизация как категория общественной науки // Общественные науки и современность. 1995. № 6 [Электронный ресурс] URL: http://ecsocman.hse.ru/data/707/717/1231/004Aleksandr_AHIEZER.pdf (дата обращения: 12.05.2016).

С учетом вышеизложенного предлагаем следующую редакцию диспозиции ч. 1 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 воздействия на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом либо физическим лицом и дестабилизации деятельности органа власти, органа местного самоуправления или международной организации*, а также угроза совершения указанных действий в тех же целях.

Идейного переосмысления требуют квалифицирующие признаки террористического акта в части установления повышенной уголовной ответственности за его совершение с использованием информационных технологий в отношении отдельных компонентов информационной среды и (или) инфраструктуры государства либо организаций. Такие предложения уже выдвигались на уровне российской доктрины. В частности, И.М. Рассолов предлагает установить повышенную уголовную ответственность за совершение террористического акта, сопряженного с несанкционированным доступом к компьютерным системам или информационно-коммуникационным сетям, осуществляющим автоматизированное управление опасными технологическими производствами и предприятиями жизнеобеспечения, с целью нарушения их функционирования и создания аварийной ситуации и угрозы техногенной катастрофы³³⁹. Однако в научной работе данного автора не дается никаких пояснений о признаках предлагаемого им состава.

О реальной возможности совершения террористического акта, связанного с разрушением информационной системы объектов

³³⁹ См.: Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. Общероссийский научно-практический правовой журнал. М.: Юрист. 2008. № 2 (134) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

инфраструктуры государства, свидетельствовали и другие исследователи³⁴⁰, однако попыток обоснования изменений в УК РФ в связи с этим не предпринималось. Кроме того, некоторые эксперты отмечают уязвимость объектов инфраструктуры государства, что обусловлено отставанием их системы безопасности от состояния информационной безопасности современного программного обеспечения³⁴¹.

Соглашаясь с И.М. Рассоловым, полагаем, что наибольшей охраны от кибертеррористических актов требуют автоматизированные системы опасных технологических производств и предприятий жизнеобеспечений, которые относятся к критически важным объектам³⁴². Не оставаясь в стороне от исследуемой проблемы, Федеральная службы по техническому и экспортному контролю России предусмотрела требования к обеспечению защиты информации в автоматизированных системах³⁴³ управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах³⁴⁴, а также объектах, представляющих повышенную опасность³⁴⁵ для жизни и здоровья людей и

³⁴⁰ См.: Капитонова Е.А. Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2015. № 2 (34). С. 32.

³⁴¹ См.: Информационная безопасность критически важных объектов [Электронный ресурс]. URL: http://www.it.ru/press_center/publications/7353/ (дата обращения: 16.11.2015).

³⁴² См.: Глава 2 §3.

³⁴³ Автоматизированные системы – это системы, состоящие из персонала и комплекса средств автоматизации его деятельности, реализующие информационную технологию выполнения установленных функций. См.: ГОСТ 34.003-90. Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения (утв. и введен в действие Постановлением Госстандарта СССР от 27.12.1990 № 3399) // М.: Стандартинформ, 2009 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

³⁴⁴ Потенциально опасный объект – объект, на котором используют, производят, перерабатывают, хранят или транспортируют радиоактивные, пожаровзрывоопасные, опасные химические и биологические вещества, создающие реальную угрозу возникновения источника чрезвычайной ситуации. См.: ГОСТ Р 22.0.02-94. Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий (принят Постановлением Госстандарта РФ от 22.12.1994 №327) (ред. от 31.05.2000) // М.: Издательство стандартов, 1995 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс»

³⁴⁵ Понятие объектов, представляющих повышенную общественную опасность, в законодательстве не раскрывается. Чаще всего используются такие понятия, как «источник повышенной опасности» или «деятельность, создающая повышенную опасность для окружающих». Последние понятия также четко не определены законодателем, лишь указывается следующее: деятельность, создающая опасность для окружающих, – это деятельность, осуществление которой создает повышенную вероятность причинения вреда из-за невозможности полного контроля над ней со стороны человека, а также деятельность по использованию, транспортировке, хранению предметов, веществ и других объектов производственного, хозяйственного или иного назначения, обладающих такими же свойствами. Причем суд по своему усмотрению сам может определить ту или иную деятельность в качестве деятельности, создающей опасность для окружающих. См.: Постановление Пленума Верховного суда РФ от 26.01.2010 № 1 «О

для окружающей природной среды³⁴⁶. По нашему мнению, вопрос о соотношении, в частности, таких объектов, как потенциально опасные и представляющие повышенную опасность, довольно спорный, поскольку в законодательстве на сегодняшний день отсутствует четкое определение последнего. Однако данная проблема требует более детального рассмотрения вне рамок настоящего диссертационного исследования.

Имея в виду, что доступность многих информационных технологий позволяет потенциальным преступникам быстро и безопасно проникать в различные информационные системы, а последствия такого проникновения в автоматизированные системы критически важных объектов и потенциально опасных объектов может превышать возможные последствия традиционного террористического акта, предлагаем дополнить ч. 2 ст. 205 УК РФ пунктом «г» следующего содержания:

сопряженные с посягательством на автоматизированные системы критически важных объектов и (или) потенциально опасных объектов государства, создающие опасность гибели человека, причинения значительного имущественного ущерба, аварийной ситуации, техногенной аварии либо иных тяжких последствий с помощью информационных технологий, - наказываются... (далее по тексту).

Понятия значительного имущественного ущерба и иных тяжких последствий раскрываются в Постановлении Пленума ВС РФ от 09.02.2012 № 12.

Понятие аварийной ситуации в автоматизированных системах управления дается ГОСТом 24.701-86. Под ней понимается некоторое исключительное состояние системы, представляющее собой определенное сочетание отказов и (или) ошибок функционирования ее элементов и

применении судами гражданского законодательства, регулирующего отношения по обязательствам вследствие причинения вреда жизни или здоровью граждан» // Рос. газета. 2010. 05 февр.

³⁴⁶ Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» // Рос. газета. 2014. 06 авг.

способное привести к нарушениям функционирования объекта управления, сопряженным с особо значительными техническими, экономическими или социальными потерями³⁴⁷.

Техногенная авария – это опасное техногенное происшествие, создающее на объекте, определенной территории или акватории угрозу жизни и здоровью людей и приводящее к разрушению зданий, сооружений, оборудования и транспортных средств, нарушению производственного или транспортного процесса, а также к нанесению ущерба окружающей природной среде³⁴⁸.

Кроме того, в некотором пояснении нуждается установление такого признака объективной стороны предлагаемого состава, как способ совершения преступления. Как было отмечено ранее, российский законодатель в ряде случаев устанавливает повышенную уголовную ответственность за совершение деяний с использованием информационно-телекоммуникационной сети (в том числе сети Интернет). Последняя же является частью понятия «информационные технологии», которое включает и технические устройства, и иные средства поиска, хранения, обработки, распространения электронной информации и т.п.³⁴⁹ Несмотря на необходимость единообразного установления квалифицирующих признаков хотя бы в определенной группе преступлений (в частности, преступлений террористической направленности), считаем обоснованным в предлагаемом составе расширение данного признака до информационных технологий. Это позволит относить к ним и иные устройства, средства, методы, процессы обработки, распространения электронной информации, не входящие в понятие информационно-телекоммуникационной сети, использование

³⁴⁷ ГОСТ 24.701-86. Государственный стандарт Союза ССР. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения (утв. и введен в действие Постановлением Госстандарта СССР от 31.03.1986 № 850 // М.: Издательство стандартов, 1986 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

³⁴⁸ ГОСТ Р 22.0.02-94. Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий (принят Постановлением Госстандарта РФ от 22.12.1994 № 327) (ред. от 31.05.2000) // М.: Издательство стандартов, 1995 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

³⁴⁹ См. подробнее Главу 2 §2.

которых может также привести к серьезным негативным последствиям (данные выводы также подтверждаются проведенным интервьюированием специалистов в области уголовного права и криминологии³⁵⁰).

Предлагаемый нами состав преступления позволит обеспечить уголовно-правовую охрану автоматизированных систем критически важных объектов и потенциально опасных объектов от террористических проявлений.

Между тем террористическая деятельность в киберпространстве не ограничивается совершением кибертеррористических актов и может также выражаться в совершении действий, направленных на поиск информации об объектах, о людях, сооружениях, мероприятиях, на финансирование терроризма и т.п.³⁵¹ Речь, в частности, идет о противоправном использовании электронной информации в киберпространстве.

На сегодняшний день уголовно-правовое законодательство России обеспечивает защиту только компьютерной информации³⁵². Глава 28 УК РФ («преступления в сфере компьютерной информации») представлена тремя статьями: ст. 272 – «неправомерный доступ к компьютерной информации», ст. 273 – «создание, использование и распространение вредоносных компьютерных программ», ст. 274 – «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»³⁵³.

³⁵⁰ См.: Прил. 5. С. 265.

³⁵¹ См.: Глава 2 §3.

³⁵² Киберпреступление – это преступление, связанное с использованием компьютеров, информационных технологий и глобальных сетей. Компьютерные преступления – преступления, совершаемые против компьютеров или компьютерных данных. См.: Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 47.

³⁵³ Впервые законодательное закрепление данная группа преступлений получила с вступлением в законную силу УК РФ 1996 года и с тех пор претерпела не мало изменений. Содержащиеся в данной главе составы не раз становились объектом научных исследований. См.: Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерной информации: дис. ... канд. юрид. наук. Саратов, 2002; Айсанов Р.М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном законодательстве: дис. ... канд. юрид. наук. М., 2006; Маляров А.И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации: автореф. дис. ... канд. юрид. наук. Краснодар, 2008; Менжега М.М. Криминологические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: дис. ... канд. юрид. наук. Саратов, 2005; Мальковцев М.М. Уголовная

Детальный анализ названных составов не входит в задачу автора данной работы и требует самостоятельного изучения. Представляется необходимым лишь обратиться к содержанию ст. 272 и 273 УК РФ в связи с включением нового квалифицирующего признака – с целью скрыть другое преступление или облегчить его совершение.

Ряд авторов, руководствуясь зарубежным опытом развития законодательства в сфере обеспечения охраны компьютерной информации, уже выдвигали подобные предложения. В частности, К.Н. Евдокимов, М.М. Менжега, М.М. Малыковцев, В.Г. Степанов-Егиянц полагают, что установление повышенной уголовной ответственности за совершение преступлений, предусмотренных ст. 272 и 273 УК РФ, с вышеуказанными целями позволит осуществлять всестороннюю и полную квалификацию данных составов³⁵⁴. В частности, К.Н. Евдокимов указывает на то, что преступления в сфере компьютерной информации часто выступают способом совершения хищения, государственной измены, шпионажа и т.п.³⁵⁵.

Такие несанкционированные вмешательства могут сопровождаться нанесением огромного экономического ущерба крупным организациям, а также способствовать раскрытию конфиденциальной информации (например, сведений, составляющих коммерческую, банковскую и иные виды тайн).

Несколько лет назад в результате кибератаки преступник получил информацию о социальном страховании, банковских счетах и кредитах, которые он опубликовал в сети Интернет. В числе пострадавших были названы директор ФБР, генеральный прокурор, начальник полиции Лос-

ответственность за создание, использование и распространения вредоносных программ для ЭВМ: дис. ... канд. юрид. наук. М., 2007.

³⁵⁴ См.: Евдокимов К.Н. Проблема уголовно-правовой квалификации преступлений в сфере компьютерной информации // Российский следователь. 2012. № 6. С. 20; Менжега М.М. Указ. соч. С. 64; Малыковцев М.М. Указ. соч. С. 115-116; Степанов-Егиянц В.Г. Субъективная сторона компьютерных преступлений // Бизнес в законе. Экономико-юридический журнал. 2013. № 2. С. 74.

³⁵⁵ См.: Евдокимов К.Н. Указ. соч. С. 20.

Анджелеса и другие³⁵⁶. В 2014 г. году хакеры взломали систему безопасности «Приват-банка» и выложили в сеть персональные банковские данные клиентов³⁵⁷.

О повышенной общественной опасности неправомерного доступа к компьютерной информации, преследующего цель совершить или облегчить совершение другого преступления, свидетельствует также анализ имеющейся судебной практики. Так, А.Н. Белко приобрел программу, предназначенную для несанкционированной аутентификации на почтовых сервисах. В результате ее использования незаконно получил номер счета и почтовые данные Ф. и перевел на свой электронный кошелек Яндекс.Деньги денежные средства в размере 20 000 рублей. Советский районный суд г. Брянска признал А.Н. Белко виновным в совершении преступлений, предусмотренных п. «в» ч. 2 ст. 158 УК РФ, ч. 2 ст. 272 УК РФ, ч. 2 ст. 273 УК РФ³⁵⁸. Таким образом, А.Н. Белко приобрел специальную программу, нейтрализующую средства защиты информации, осуществил неправомерный доступ к компьютерной информации в целях совершения хищения.

Также неправомерный доступ к компьютерной информации может преследовать цель совершения преступления, предусмотренного ст. 183 УК РФ («незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»)³⁵⁹.

Между тем совершение компьютерных преступлений, связанных с неправомерным доступом к охраняемой законом информации, может облегчить совершение и террористических преступлений. Об этом

³⁵⁶ См.: Хакер выложил в сеть финансовые данные американских знаменитостей и политиков, в их числе директор ФБР [Электронный ресурс]. URL: http://www.gazeta.ru/social/news/2013/03/12/n_2794737.shtml (дата обращения: 17.05.2016).

³⁵⁷ См.: Данные клиентов «Приват-банка» выложили в Сеть [Электронный ресурс]. URL: <https://life.ru/t/новости/135943> (дата обращения 17.05.2016).

³⁵⁸ См.: Приговор Советского районного суда г. Брянска № 1-262/2015 от 14 августа 2015 года по делу № 1-262/2015 [Электронный ресурс]. URL: <http://sudact.ru/regular/doc/Nw3su7zzqdZC/> (дата обращения: 17.05.2016).

³⁵⁹ См.: Приговор Невельского районного суда Псковской области № 1-20/2015 от 12 марта 2015 года по делу № 1-20/2015 [Электронный ресурс]. URL: <http://sudact.ru/regular/doc/lqcdM5fJ1fLc/> (дата обращения: 17.05.2016).

свидетельствуют исследования, проводимые зарубежными специалистами в области противодействия терроризму³⁶⁰.

По данным некоторых СМИ, цитировавших заместителя постоянного представителя Ирана в ООН, серия террористических актов в отношении физиков-ядерщиков, работавших над иранской ядерной программой, аспиранта, который трудился над детонатором будущей иранской атомной бомбы, была результатом неправомерного вмешательства в компьютерные системы МАГАТЭ, содержащие информацию о местонахождении указанных лиц³⁶¹.

Несмотря на различия в правовых системах, следует, на наш взгляд, обратить внимание на положительный опыт законодательного закрепления исследуемого квалифицирующего признака в Великобритании. Закон о злоупотреблении компьютером (Computer Misuse Act 1990) в ст. 2 (1) предусматривает ответственность за «незаконный доступ лица к компьютерным материалам с намерением совершить или облегчить (такому лицу или иным лицам) совершение последующих преступлений»³⁶². Согласно закону при совершении последующих преступлений дальнейшее использование компьютера необязательно³⁶³.

Кроме того, ст. 58 Закона о терроризме 2000 года устанавливает ответственность за сбор, изготовление и хранение информации, которая может быть полезна для совершающегося или готовящегося к совершению террористического акта³⁶⁴. При этом суд присяжных обязан установить так называемый «критерий практической пользы» такой информации³⁶⁵.

³⁶⁰ См.: Использование Интернета в террористических целях // Управление Организации Объединенных Наций по наркотикам и преступности. Нью-Йорк, 2013. С. 10 [Электронный ресурс]. URL: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf (дата обращения: 21.05.2016).

³⁶¹ См.: Бондарь Ю.М. Указ. соч. [Электронный ресурс]. URL: <http://www.iimes.ru/rus/stat/2012/27-02-12d.htm> (дата обращения: 21.05.2016).

³⁶² См.: Computer Misuse Act 1990 [Электронный ресурс]. URL: <http://www.legislation.gov.uk/ukpga/1990/18/section/2> (дата обращения: 27.05.2016).

³⁶³ См.: Уголовное право зарубежных стран. Общая и Особенная части: учебник для магистров / Н.А. Голованова, Е.В. Еремин, М.А. Игнатова [и др.]; под ред. Н.Е. Крыловой. 4-е изд., перераб. и доп. М.: Юрайт, 2013. С. 633.

³⁶⁴ См.: Использование Интернета в террористических целях // Управление Организации Объединенных Наций по наркотикам и преступности. Нью-Йорк, 2013. С. 33 [Электронный ресурс]. URL:

Между тем исследователи проблем компьютерного законодательства в Республике Молдова также свидетельствуют о все более частом осуществлении неправомерного доступа к охраняемой компьютерной информации и распространения вредоносных компьютерных программ с целью совершения другого преступления³⁶⁶.

Уголовному законодательству РФ известно такое обстоятельство отягчающее наказание, как совершение преступления «с целью скрыть другое преступление или облегчить совершение другого преступления». В качестве квалифицирующего признака данное обстоятельство предусматривается п. «к» ч. 2 ст. 105 («убийство») и ч. 2 ст. 327 («подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков») УК РФ, что обусловлено спецификой данных составов, а также их общественной опасностью. Для всех остальных составов, предусмотренных Особенной частью УК РФ, данное обстоятельство может учитываться как отягчающее и влиять на размер, срок и вид наказания с учетом положений Общей части УК РФ.

Однако установление исследуемого обстоятельства как отягчающего для тех составов, где оно не предусмотрено в качестве квалифицирующего признака, связано с определенными трудностями в назначении наказания, поскольку Общая часть УК РФ не предусматривает правил усиления наказания при наличии обстоятельств, предусмотренных ст. 63 УК РФ³⁶⁷.

Диссертант также полагает, что выделение такого обстоятельства в качестве квалифицирующего признака составов преступлений, предусмотренных ст. 272, 273 УК РФ, необходимо в связи с их

https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf (дата обращения: 21.05.2016).

³⁶⁵ См.: Там же. С. 33.

³⁶⁶ См.: Лазарева Н. Уголовно-правовая характеристика преступлений в области информатики и электросвязи // Studia Universitatis. 2007. С. 138.

³⁶⁷ О проблемах влияния наличия отягчающих обстоятельств, предусмотренных ст. 63 УК РФ, на назначение наказания См.: Пилипенко С.П. Институт обстоятельств, отягчающих наказание, в уголовном законодательстве (теоретико-прикладной анализ): автореф. дис. ... канд. юрид. наук. Н. Новгород, 2007. С. 14-16.

особенностью³⁶⁸, обусловленной доступностью киберпространства. За 2014 год МВД зарегистрировано около 11 000 преступлений, предусмотренных гл. 28 УК РФ³⁶⁹ (для сравнения за 11 месяцев 2011 года было зарегистрировано 120 преступлений³⁷⁰), что свидетельствует о возрастающей угрозе использования киберпространства злоумышленниками.

На уровне доктрины уже предпринимались попытки определения степени общественной опасности, в частности неправомерного доступа к охраняемой законом компьютерной информации, совершенного с целью скрыть другое преступление или облегчить его совершение. К.Н. Евдокимов определил его «место» в ч. 2 ст. 272 УК РФ³⁷¹. Данное представление об общественной опасности исследуемого признака мы считаем допустимым. Однако в другой (более поздней) научной публикации К.Н. Евдокимов совместно с С.В. Пархоменко предлагает поместить исследуемый признак в ч. 3 ст. 272 и ч. 2 ст. 273 УК РФ с установлением максимального наказания до десяти лет лишения свободы³⁷². Последняя позиция объясняется авторами тем, что преступления в сфере компьютерной информации часто выступают или могут стать способом совершения других тяжких и особо тяжких преступлений³⁷³.

В Великобритании за совершение неправомерного доступа к охраняемой законом компьютерной информации с целью скрыть другое

³⁶⁸ В этом мы солидарны с позицией М.М. Менжега. См.: Менжега М.М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: дис. ... канд. юрид. наук. Саратов, 2005. С. 68.

³⁶⁹ См.: МВД Зарегистрировало около 11 000 киберпреступлений в 2014 г. [Электронный ресурс] URL: <http://www.vedomosti.ru/technology/articles/2015/02/06/kiberprestupniki-v-spiskah-ne-znachatsya> (дата обращения: 17.11.2015).

³⁷⁰ См.: Мухачев С.В. Динамика информационных компьютерных преступлений // Совершенствование и внедрение IT-технологий в деятельности органов внутренних дел Российской Федерации [Электронный ресурс]. URL: <http://www.mvd.informost.ru/2012/pdf/part1/1-27.pdf> (дата обращения: 17.11.2015).

³⁷¹ См.: Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации (по материалам Восточно-Сибирского региона): дис. ... канд. юрид. наук. Иркутск, 2006. С. 13.

³⁷² См.: Пархоменко С.В. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подход // Криминологический журнал Байкальского государственного университета экономики и права. 2015, Т. 9. № 2. С. 271.

³⁷³ См.: Пархоменко С.В. Указ соч. С. 7.

преступление или облегчить его совершение предусматривается ответственность до пяти лет тюремного заключения³⁷⁴.

Представляется возможным с учетом вышеизложенного определить «место» исследуемого признака в ч. 2 ст. 272 УК РФ, и изложить ее в следующей редакции:

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, а равно с целью скрыть другое преступление или облегчить его совершение, - наказывается ...

При этом считаем необходимым переосмыслить содержание ст. 273 УК РФ и привести ее в соответствие со ст. 272 УК РФ в части определения в качестве квалифицирующих и особо квалифицирующих некоторых криминообразующих признаков. В соответствии с действующим законодательством общественная опасность преступления, предусмотренного ст. 273 УК РФ, несколько выше (основной состав предусматривает максимальное наказание до четырех лет лишения свободы; для сравнения ч. 1 ст. 272 УК РФ предусматривает максимальное наказание до двух лет лишения свободы), чем неправомерного доступа к охраняемой законом компьютерной информации. Такое законодательное решение уже не раз вызывало сомнения у ряда исследователей, характеризующих вредоносность рассматриваемых преступлений как вполне сопоставимую³⁷⁵. Пытаясь определить адекватность установленного санкцией ч. 1 ст. 273 УК РФ максимального размера наказания в виде лишения свободы, Е. Новикова соотнесла данное преступление с умышленным уничтожением и повреждением имущества, предусмотренного ч. 1 ст. 167 УК РФ (максимальный размер наказания в виде лишения свободы – два года). В заключение автор приходит к выводу, что единственным основанием большей общественной опасности преступления, предусмотренного ст. 273

³⁷⁴ См.: Уголовное право зарубежных стран. Общая и Особенная части: учебник для магистров / Н.А. Голованова, Е.В. Еремин, М.А. Игнатова [и др.]; под ред. Н.Е. Крыловой. 4-е изд., перераб. и доп. М.: Юрайт, 2013. С. 633.

³⁷⁵ См.: Лопашенко Н.А. Основы уголовно-правового воздействия: уголовное право, уголовный закон, уголовно-правовая политика. СПб.: Юридический центр Пресс, 2004. С. 311.

УК РФ, может быть только специальный субъект, поскольку, по ее мнению, лишь лицо, обладающее специальными знаниями, способно совершить подобное преступление³⁷⁶. Однако представляется невозможным признать это существенным аргументом.

На сегодняшний день общественная опасность преступления, предусмотренного ч. 1 ст. 273 УК РФ, равна общественной опасности ч. 3 ст. 109 УК РФ («причинение смерти двум или более лицам по неосторожности»). Подобное законодательное решение в отношении санкции ч. 1 ст. 273 УК РФ, а равно квалифицирующих и особо квалифицирующих признаков, нельзя признать удачным.

Анализ норм зарубежного законодательства, предусматривающих ответственность за использование или распространение вредоносных программ, также свидетельствует о завышенной общественной опасности данного состава в УК РФ.

Так, ст. 361-1 УК Украины³⁷⁷ и ст. 278⁶ УК Республики Узбекистан³⁷⁸ за данное преступление по основному составу предусматривают максимальное наказание в виде лишения свободы сроком до двух лет.

Кроме того, некоторые сомнения вызывает различное определение степени общественной опасности одинаковых по существу криминообразующих признаков составов преступлений, предусмотренных ст. 272 и 273 УК РФ.

Часть 2 ст. 273 УК РФ устанавливает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, совершенных группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего

³⁷⁶ См.: Новикова Е. Использование ограничения свободы в санкциях за преступления в сфере компьютерной информации [Электронный ресурс]. URL: https://zakon.ru/blog/2012/2/26/ispolzovanie_ogranicheniya_svobody_v_sankciyah_za_prestupleniya_v_sfere_kompyuternoj_informacii (дата обращения: 23.05.2016).

³⁷⁷ Уголовный кодекс Украины (с изм. и доп. от 15.03.2016) [Электронный ресурс]. URL: <http://meget.kiev.ua/kodeks/ugolovnij-kodeks/> (дата обращения: 23.05.2016).

³⁷⁸ Уголовный кодекс Республики Узбекистан [Электронный ресурс]. URL: http://lex.uz/pages/getact.aspx?act_id=111457 (дата обращения: 23.05.2016).

служебного положения, а равно причинивших крупный ущерб или совершенных из корыстной заинтересованности. При этом максимальное наказание за данные преступления установлено в виде лишения свободы до пяти лет. Как видится, аналогичные признаки, отягчающие наказание, содержатся в частях 2, 3 ст. 272 УК РФ, дифференцируя максимальное наказание соответственно до четырех и пяти лет лишения свободы. Считаем недопустимым определять в одной группе преступлений различную степень общественной опасности одних и тех же квалифицирующих признаков.

Кроме того, анализ 60 приговоров районных и городских судов Кировской области, Красноярского края, Удмуртской Республики, Московской, Тюменской областей и других по 69 эпизодам совершения преступлений по ч. 1 и ч. 2 ст. 273 УК РФ за 2015 г. по май 2016 г. показал следующее.

В 54% случаев по ч. 1 ст. 273 УК РФ назначается наказание в виде лишения свободы (в 100 % случаев суд постановляет считать назначенное наказание условным), в 40 % случаев к осужденным применяется наказание в виде ограничения свободы, во всех остальных случаях (6%) назначает более мягкое наказание с применением ст. 64 УК РФ.

В 59% случаев по ч. 2 ст. 273 УК РФ назначается наказание в виде ограничения свободы, в 41% случаев к осужденным применяется наказание в виде лишения свободы (в 100% случаев суд постановляет считать назначенное наказание условным). Максимальное назначаемое наказание в виде лишения свободы на основании изученных приговоров по ч. 1 ст. 273 УК РФ составляет полтора года лишения свободы, по ч. 2 ст. 273 УК РФ – два года лишения свободы³⁷⁹.

Проведенный анализ практического применения ст. 273 УК РФ, а также доктринальные исследования в области пенализации и депенализации уголовно-правовых санкций свидетельствуют о необходимости снижения уголовной ответственности за создание, использование и распространение

³⁷⁹ См.: Прил. 4. С. 248.

вредоносных компьютерных программ, а также изменения общественной опасности некоторых криминообразующих признаков данного преступления в соответствии со ст. 272 УК РФ.

Исходя из вышеизложенного и учитывая предложение диссертанта о включении нового квалифицирующего признака в ст. 273 УК РФ, следует:

1) расположить криминообразующие признаки ст. 273 УК РФ в той же последовательности, что и в ст. 272 УК РФ, дифференцируя максимальные наказания по ч. 2 – до четырех лет лишения свободы, по ч. 3 – до пяти лет лишения свободы, по ч. 4 – до семи лет лишения свободы³⁸⁰;

2) определить признак «с целью скрыть другое преступление или облегчить его совершение» в ч. 2 ст. 273 УК РФ по аналогии со ст. 272 УК РФ и изложить его в следующей редакции.

Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, а равно с целью скрыть другое преступление или облегчить его совершение, - наказываются...

Подобные изменения, связанные с установлением в качестве квалифицирующего признака специальной цели «скрыть другое преступление или облегчить его совершение», позволят не только устранить пробел в квалификации деяний, предусмотренных статьями 272, 273 УК РФ, но и предупредить неправомерное использование компьютерных сетей для дальнейшего совершения террористических преступлений.

Между тем киберпространство используется террористами и для других целей, например для финансирования терроризма³⁸¹. Современному уголовному законодательству известно данное общественно опасное деяние, ответственность за которое устанавливается в ч. 1 ст. 205¹ УК РФ («содействие террористической деятельности»). Согласно примечанию к

³⁸⁰ В настоящее время действующим законодательством санкции статей 272 и 273 УК РФ являются альтернативными и кумулятивными. Детальное исследование вопроса депенализации санкции ст. 273 УК РФ требует более подробного рассмотрения. Однако исследование, проведенное диссертантом, может стать основой для его дальнейшего изучения.

³⁸¹ В 2015 году по фактам финансирования терроризма было возбуждено 270 уголовных дел. См.: Глава ФСБ: по фактам финансирования терроризма возбуждено 270 уголовных дел [Электронный ресурс]. URL: <http://regnum.ru/news/polit/2036140.html> (дата обращения: 24.05.2016).

статье под финансированием терроризма следует понимать предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки или совершения хотя бы одного из преступлений, предусмотренных статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 206, 208, 211, 220, 221, 277, 278, 279 и 360 УК РФ, либо для финансирования или иного материального обеспечения лица в целях совершения хотя бы одного из этих преступлений, либо для обеспечения организованной группы, незаконного вооруженного формирования, преступного сообщества (преступной организации), созданных или создаваемых для совершения хотя бы одного из этих преступлений.

На сегодняшний день нередки случаи использования информационных технологий в целях финансирования терроризма. Это обусловлено доступностью и анонимностью очень многих платежных интернет-систем (Webmoney, PayPal, Qiwi, ЯндексДеньги и т.д.), не требующих указания личных данных или регистрации. Помимо этого, террористами активно используются и простые банковские переводы³⁸²: международному сообществу известны случаи осуществления мошеннических действий с банковскими картами в целях финансирования терроризма (использования краденных реквизитов банковских карт)³⁸³.

Российское законодательство, как, впрочем, и законодательство Республики Казахстан, Украины и Республики Узбекистан, не предусматривает какого-либо усиления уголовной ответственности за финансирование терроризма с использованием информационных технологий. Нам видится такое законодательное решение вполне оправданным, несмотря

³⁸² См.: Моисеенко А.С. О противодействии использованию сети Интернет в террористических целях // Журнал «Наука и образование: хозяйство и экономика; предпринимательство; право и управление» [Электронный ресурс]. URL: http://www.journal-nio.com/index.php?option=com_content&view=article&id=3757%3A-14&catid=114%3Amar&Itemid=157 (дата обращения: 24.05.2016).

³⁸³ См.: Новые риски финансирования терроризма // Группа разработки финансовых мер борьбы с отмыванием денег ФАТФ [Электронный ресурс]. URL: http://eurasiangroup.org/ru/news/typ_14.pdf (дата обращения: 24.05.2016).

на предметную направленность данного диссертационного исследования. Это обусловлено в первую очередь всесторонним внедрением и использованием информационных технологий в финансовой сфере. Кроме того, санкция ч. 1 ст. 205 УК РФ весьма высока и предусматривает наказание до десяти лет лишения свободы (для сравнения в УК Республики Казахстан – до семи лет лишения свободы, в УК Украины – до восьми лет лишения свободы).

Несмотря на это, представители ФСБ России указывают на определенные трудности при расследовании уголовных дел по факту финансирования терроризма в сети Интернет, связанные с существующими сегодня «традиционными и правовыми рамками»³⁸⁴. Однако данная проблема больше криминалистического характера, нежели уголовно-правового.

Некоторые спорные вопросы состава финансирования терроризма были исследованы в работах П.В. Агапова, К.В. Михайлова, В.В. Ульяновой³⁸⁵. В частности, следует согласиться с выводами В.В. Ульяновой по поводу неудачности использования законодателем понятия «терроризм» в диспозиции ч. 1 ст. 205 УК РФ. Данная позиция объясняется использованием не уголовно-правового понятия терроризма в диспозициях статей УК РФ, что и, на наш взгляд, является недопустимым. После вступления в силу Федерального закона РФ № 35-ФЗ понятие «терроризм» получило другой правовой статус³⁸⁶, стало отражать сущность определенного явления. УК РФ, в свою очередь, требует конкретизации в установлении признаков любого состава преступлений. В связи с этим предложение В.В. Ульяновой о замене

³⁸⁴ См.: ФСБ попросила ужесточить законы против интернет-финансирования терроризма [Электронный ресурс]. URL: <http://www.interfax.ru/russia/479524> (дата обращения: 24.05.2016).

³⁸⁵ См.: Агапов П.В., Михайлов К.В. Уголовная ответственность за содействие террористической деятельности: тенденции современной уголовной политики. Саратов: Саратов. юрид. ин-т МВД России, 2007 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс»; Ульянова В.В. Противодействие финансированию терроризма: дис. ... канд. юрид. наук. Екатеринбург, 2010. С. 78-120.

³⁸⁶ Некоторые исследователи определяют его как криминологическое понятие. См.: Моисеенко А.И. Уголовно-правовая и криминологическая характеристика терроризма (по материалам Южного федерального округа России): дис. ... канд. юрид. наук. Ставрополь, 2006. С. 9.

понятия финансирования терроризма понятием финансирования террористической деятельности считаем вполне обоснованными³⁸⁷.

В целом же, проблемные вопросы уголовной ответственности за финансирование терроризма требуют самостоятельного изучения не в рамках данного диссертационного исследования.

Резюмируя предложенные диссертантом меры уголовно-правового противодействия информационно-технологическому терроризму, отметим, что российское законодательство в области охраны компьютерной информации, использования информационных технологий требует серьезных преобразований. Зарубежное законодательство Великобритании, США, Украины³⁸⁸, Республики Узбекистан³⁸⁹, Республики Казахстан³⁹⁰ ушло далеко вперед и может стать основой для адекватных изменений в УК РФ.

Уголовно-правовые меры противодействия информационно-психологическому терроризму.

На сегодняшний день актуальным является вопрос обеспечения защиты населения от неправомерного информационно-психологического воздействия терроризма. Глобализация информационного пространства, связанная с появлением сети Интернет и других локальных и территориальных сетей, расширила границы использования информации как инструмента психологического воздействия.

Современное российское законодательство предусматривает несколько составов, направленных на защиту населения от информационно-

³⁸⁷ См.: Ульянова В.В. Указ. соч. С. 103.

³⁸⁸ Уголовное законодательство Украины на сегодняшний день предусматривает 6 составов преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи. См.: Уголовный кодекс Украины (с изм. и доп. от 15.03.2016) [Электронный ресурс]. URL: <http://meget.kiev.ua/kodeks/ugolovniy-kodeks/> (дата обращения: 23.05.2016).

³⁸⁹ Уголовное законодательство Узбекистана предусматривает 6 составов преступлений в сфере информационных технологий, в их числе компьютерный саботаж, нарушение правил информатизации и др. См.: Уголовный кодекс Республики Узбекистан [Электронный ресурс]. URL: http://lex.uz/pages/getact.aspx?lact_id=111457 (дата обращения: 23.05.2016).

³⁹⁰ Уголовное законодательство Республики Казахстан в главе преступлений против безопасности информационных технологий предусматривает ответственность за умышленное нарушение работы информационной системы или информационно-коммуникационной сети, неправомерное завладение информацией, принуждение к передаче информации и еще 6 составов. См.: Уголовный кодекс Республики Казахстан [Электронный ресурс]. URL: http://online.zakon.kz/Document/?doc_id=1008032#pos=2807;-182 (дата обращения: 23.05.2016).

психологического воздействия терроризма. К таковым следует отнести ч. 1, ч. 2 ст. 205¹ и ст. 205² УК РФ³⁹¹.

Названные статьи были введены в УК РФ в связи с ратификацией Конвенции Совета Европы «О предупреждении терроризма»³⁹². Общим для исследуемых составов является то, что они связаны с оказанием воздействия на сознание человека (людей) и являются частными случаями подстрекательства.

Часть 1 статьи 205¹ УК РФ предусматривает ответственность за склонение, вербовку и иное вовлечение в совершение некоторых преступлений террористической направленности³⁹³.

О неудачности общего содержания ст. 205¹ УК РФ не раз уже высказывались многие российские ученые³⁹⁴. Однако задачей данного диссертационного исследования является изучение лишь тех общественно опасных деяний, которые связаны с оказанием воздействия на сознание человека (людей).

Исходя из содержания ч. 1 ст. 205¹ УК РФ склонение и вербовка являются разновидностями вовлечения лица в совершение указанных в диспозиции преступлений. Постановление Пленума ВС РФ от 09.02.2012 № 12 не дает разъяснения о сущностном содержании каждого из указанных деяний, характеризуя их в общем как умышленные действия, направленные на вовлечение лица в совершение одного или нескольких указанных преступлений, например путем уговоров, убеждения, просьб, предложений,

³⁹¹ Однако ч. 2 ст. 205¹ УК РФ не требует детального рассмотрения в рамках данного диссертационного исследования, поскольку указывает на квалифицирующий признак интересующего нас состава – ч. 1 ст. 205¹ УК РФ.

³⁹² См.: Федеральный Закон от 27.07.2006 № 153-ФЗ (с изм. и доп. от 06.07.2016, № 375-ФЗ) «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального Закона "О ратификации Конвенции Совета Европы о предупреждении терроризма" и Федерального Закона "О противодействии терроризму"» // СЗ РФ. 2006. № 35 (1 ч.), ст. 3452; 2016. № 28, ст. 4559.

³⁹³ Указанные деяния являются альтернативными по отношению к финансированию терроризма, исследованному ранее в рамках данного диссертационного исследования, а также вооружению и подготовке в целях совершения одного из указанных в диспозиции преступлений.

³⁹⁴ См.: Агапов П.В., Михайлов К.В. Указ. соч. [Электронный ресурс]. Доступ из СПС «КонсультантПлюс»; Кочои С.М. Общеевропейское законодательство о борьбе с терроризмом и перспективы реформирования УК РФ // Lex Russica. 2014. №9 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

применения физического воздействия или посредством поиска лиц и вовлечения их в совершение хотя бы одного из указанных преступлений.

В связи с отсутствием единства в понимании терминов «вовлечение», «склонение» и «вербовка» среди исследователей возникают споры о синонимичности некоторых из них.

На проблемы соотношения данных понятий и их сущностного содержания указывали такие ученые, как В.Л. Кудрявцев, В.В. Палий, Ю.В. Радостева, Н.Н. Бугера, П.В. Агапов, К.В. Михайлов и др.³⁹⁵

Соотношение понятий «вовлечение» и «склонение».

Некоторые исследователи полагают, что данные понятия в большей степени являются совпадающими (Ю.В. Радостева)³⁹⁶. В.Л. Кудрявцев же отмечает, что подобный вывод исходит из содержания Постановления Пленума ВС РФ от 09.02.2012 № 12³⁹⁷.

Другим же представляется, что понятие «вовлечение» – более широкое, нежели понятие «склонение»³⁹⁸. Вовлечение может выражаться как в психологическом (информационном), так и в физическом воздействии. Склонение, в свою очередь, – форма вовлечения, представляющая собой психологическое (информационное) воздействие³⁹⁹. Данную точку зрения подтверждают и некоторые практические примеры. Так, приговором Волгоградского областного суда от 1 марта 2013 года А.А. Быкова признана виновной в содействии террористической деятельности, выразившемся в склонении путем уговоров и предложении другому лицу с целью вступления

³⁹⁵ См.: Кудрявцев В.Л. Склонение, вербовка или иное вовлечение лица как альтернативные действия объективной стороны содействия террористической деятельности // Адвокат. 2012. № 5. С. 21; Палий В.В. Вовлечение в совершение преступления и склонение к совершению преступлений или антиобщественных действий: автореф. ... канд. юрид. наук. М., 2006. С. 9; Радостева Ю.В. Указ. соч. С. 112; Бугера Н.Н. Соотношение понятий «вовлечение» и «склонение» в уголовном праве России // Юридическая наука и правоохранительная практика. 2014. № 3 (29). С. 38.; Агапов П.В., Михайлов К.В. Указ. соч. [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

³⁹⁶ См.: Радостева Ю.В. Указ. соч. С. 112.

³⁹⁷ См.: Кудрявцев В.Л. Указ. соч. С. 21.

³⁹⁸ См.: Бугера Н.Н. Указ. соч. С. 39.

³⁹⁹ См.: Палий В.В. Указ. соч. С. 9.

в незаконное вооруженное формирование⁴⁰⁰. Приговором от 14 мая 2014 года Х.Ф. Турсунов признан виновным в содействии террористической деятельности, выразившемся в склонении другого лица к совершению террористического акта через социальную сеть «Одноклассники»⁴⁰¹.

Таким образом, склонение выражается в совершении действий, связанных с психологическим воздействием на склоняемое лицо.

Соотношение понятий «склонение» и «вербовка».

Ряд авторов полагают, что вербовка является способом склонения⁴⁰².

Другие, напротив, различают данные понятия. Вербовка, по мнению Г.Г. Криволапова, состоит в привлечении (найме) лиц, самостоятельно изъявивших желание участвовать в совершении преступлений⁴⁰³. Подобного же мнения придерживается и В.Л. Кудрявцев, приводя некоторые примеры из судебной практики⁴⁰⁴. Вербовка в отличие от склонения, таким образом, не предусматривает психологического воздействия на вербуемое лицо⁴⁰⁵. Представляется, что вербовка является самостоятельной формой вовлечения.

Исходя из вышеизложенного представляется допустимым использование в качестве объективных признаков исследуемого состава указание на три деяния – склонение, вербовку и иное вовлечение. Это объясняется неидентичностью исследованных терминов, возможно и совпадающих в определенной части (имеются в виду понятия «склонение» и «вовлечение», «вербовка» и «вовлечение»).

Между тем неясным остается вопрос о перечне преступлений, склонение (вербовка и иное вовлечение) к которым влечет уголовную

⁴⁰⁰ См.: Данные из Апелляционного определения Верховного суда РФ по делу № 16-АПУ13-3, г. Москва, 16 мая 2013 [Электронный ресурс]. URL: http://www.vsrp.ru/stor_pdf.php?id=540406 (дата обращения: 25.05.2016).

⁴⁰¹ См.: Приговор №1-248/2014 от 14 мая 2014 г. в отношении Турсунова Х.Ф [Электронный ресурс]. URL: <http://sudact.ru/regular/doc/2tLvc18w88N8/> (дата обращения: 25.05.2016).

⁴⁰² Цит. по: Нагаева Т.А. Применение терминов «вовлечение» и «склонение» в Российском уголовном праве // Lex Russica. 2011. № 3. С. 528.

⁴⁰³ См.: Уголовное право. Общая и Особенная части: учебник / К.Л. Акоев, С.И. Никулин, А.Е. Беляева [и др.]; под ред. М.П. Журавлева, С.И. Никулина. М., 2007. С. 536.

⁴⁰⁴ См.: Кудрявцев В.Л. Указ. соч. С. 23.

⁴⁰⁵ См.: Уголовное право Особенная часть: учебник для бакалавров / Ю.В. Грачева, А.И. Рарог, В.В. Палий; под ред. А.И. Чучаева. М.: Проспект, 2013 [Электронный ресурс]. URL: https://books.google.ru/books?id=FSw_Zrz-k7UC&printsec=frontcover&hl=ru#v=onepage&q&f=false (дата обращения: 25.05.2016).

ответственность. К таковым отнесены ст. 205, 205², 205³, 205⁴, 205⁵, 206, 208, 211, 220, 221, 277, 278, 279, 360 и 361 УК РФ.

Как было отмечено ранее, снова без внимания остается вопрос возможности привлечения к уголовной ответственности за вовлечение лица в целях финансирования террористической деятельности (между тем последние изменения позволяют привлекать к уголовной ответственности за склонение (вербовку или иное вовлечение) лица в целях финансирования акта международного терроризма), хотя об опасности подобного рода деяний свидетельствуют некоторые исследования. В частности, вовлечение некоммерческих организаций в незаконную деятельность, связанную с финансированием, представляет собой серьезную угрозу⁴⁰⁶.

Возвращаясь к разъяснениям Постановления Пленума ВС РФ от 09.02.2012 № 12, обратим также внимание на то, что действия ч. 1 ст. 205¹ УК РФ охватывают и случаи размещения и распространения просьб, уговоров, предложений и прочего в информационно-телекоммуникационной сети. Несмотря на то что данный признак – использование информационно-телекоммуникационной сети (в том числе сети Интернет) – во многих составах УК РФ определяется в качестве квалифицирующего, считаем целесообразным не вводить его в ст. 205¹ УК РФ, поскольку санкция часть 1 исследуемой статьи весьма высока и предусматривает наказание до десяти лет лишения свободы (для сравнения: ст. 258¹ УК Украины «вовлечение в совершение террористического акта» предусматривает максимальное наказание до пяти лет лишения свободы).

В 2006 году Федеральным законом «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О ратификации Конвенции Совета Европы о предупреждении трероризма" и Федерального закона "О противодействии терроризма"» в УК РФ была введена ст. 205² («публичные призывы к

⁴⁰⁶ См.: Новые риски финансирования терроризма. Указ. соч. С. 21 [Электронный ресурс]. URL: http://www.cbr.ru/today/anti_legalisation/fatf/Emerging-Terrorist-Financing-Risks-Russian.pdf (дата обращения: 25.05.2016).

осуществлению террористической деятельности или публичное оправдание терроризма»). Данная статья является интерпретацией одного из положений Конвенции Совета Европы «О предупреждении терроризма» – «публичное подстрекательство к совершению террористического преступления»⁴⁰⁷.

Общественная опасность исследуемого преступления, безусловно, велика, поскольку оно направлено в первую очередь на формирование терпимости к действиям террористов, понимания, сочувствия к их взглядам и преследуемым целям, подрыв доверия населения к органам власти, преследующим антитеррористическую политику. Криминализация данного деяния направлена на предотвращение распространения терроризма и идеологии насилия, лежащей в основе данного негативного явления.

Однако на сегодняшний день исследователи в области уголовно-правового противодействия терроризму уже не раз отмечали несовершенство конструкции этой нормы, создающее проблемы в квалификации деяний по ст. 205² УК РФ, а также несоответствие исследуемой нормы современным тенденциям развития информационных технологий⁴⁰⁸. Сказанное свидетельствует о необходимости подвергнуть критическому анализу все четыре элемента состава преступления, предусмотренного ст. 205² УК РФ.

Непосредственным объектом данного преступления, как и преступления, предусмотренного ст. 205 УК РФ, является общественная безопасность.

Объективная сторона состава преступления, предусмотренного ч. 1 ст. 205² УК РФ, характеризуется альтернативными действиями:

- 1) публичным оправданием терроризма;
- 2) публичными призывами к осуществлению террористической деятельности.

⁴⁰⁷ См.: Конвенция Совета Европы «О предупреждении терроризма» (CETS № 196) [рус., англ.] (заключена в г. Варшаве 16.05.2005) // СЗ РФ. 2009. № 20, ст. 2393.

⁴⁰⁸ См.: Пинкевич Т.В. Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма: проблемы квалификации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2014. № 3. С. 141-144; Фарвазова Ю.Р. Актуальные аспекты совершенствования правового регулирования незаконного использования информационного пространства в террористических целях // Армия и общество. 2013. № 5. С. 18-22.

Постановление Пленума ВС РФ от 09.02.2012 № 12, а также примечание 1 к ст. 205² УК РФ разъясняют понятия, составляющие объективную сторону данного преступления: публичное оправдание и публичные призывы.

Публичное оправдание терроризма выражается в заявлении о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании.

При анализе сущностного содержания исследуемого деяния обнаруживаются следующие проблемы: во-первых, содержание понятия «оправдание» раскрывается через «заявление о признании». Толковый словарь русского языка раскрывает понятие заявления как официальное обращение в письменной или устной форме либо как письменную просьбу о чем-либо⁴⁰⁹. Предполагается, что такое заявление так или иначе должно иметь какую-либо официальную форму, быть недвусмысленным и четко выражать мысль субъекта о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании.

Те же толковые словари раскрывают понятие «оправдание» через понятие «признание», поэтому толкование исследуемого понятия как заявления о признании представляется необоснованно пространным, достаточно говорить только о *публичном признании*.

При определении сущности оправдания терроризма используется словосочетание «идеология терроризма»⁴¹⁰, однако его содержание и «природа» не разъясняются⁴¹¹. Этот вопрос тем более актуален в связи с тем, что в ст. 3 Федерального закона «О противодействии терроризму» при

⁴⁰⁹ См.: Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. М.: Азбуковник, 1999. С. 226; Словарь Ожегова. Толковый словарь русского языка [Электронный ресурс] URL: <http://www.ozhegov.com/> (дата обращения: 14.01.2015).

⁴¹⁰ Исходя из положений ст. 3 Федерального Закона № 35-ФЗ «О противодействии терроризму» идеологию терроризма следует буквально понимать как идеологию идеологии и практики применения насилия...

⁴¹¹ Проведенное диссертантом исследование понятия терроризм (См. Глава 1 §1) определяет идеологию как основу терроризма. В таком случае следует говорить об идеологии, составляющей основу терроризма, но не об идеологии терроризма.

раскрытии сущности терроризма используется словосочетание «идеология насилия».

Кроме того, представляется неудачным использование не уголовно-правового понятия «терроризм» в диспозициях статей УК РФ, в том числе и в ст. 205² УК РФ⁴¹². В связи с этим, следует говорить не о публичном оправдании терроризма, а о *публичном оправдании террористической деятельности*. Анализ судебной практики показал, что виновные признавали в качестве правильной деятельность, выражающуюся в совершении ими преступлений террористической направленности. В частности, приговором Ивановского районного суда Ивановской области №1-207/2010 по делу № 1-207/2010 установлено, что «у Н.А. Кувакиной возник умысел на оказание публичной поддержки террористической деятельности представителей незаконных вооруженных формирований на территории Северного Кавказа»⁴¹³.

Приговором Ленинского районного суда г. Кирова № 1-586/2010 в отношении И.В. Михеева установлено, что последний, обращаясь к большому количеству граждан – участникам митинга, публично произнес лозунг, восхвалявший другое лицо, взорвавшее рынок и признанное виновным в ряде преступлений, в том числе по ч. 3 ст. 205 УК РФ⁴¹⁴. Тем самым исходя из содержания приговора И.В. Михеев оправдал террористическую деятельность данного лица, выразившуюся в совершении террористического акта.

Второе альтернативное деяние согласно диспозиции ч. 1 ст. 205² УК РФ предполагает совершение публичного призыва к осуществлению террористической деятельности. Установление за него уголовной ответственности породило некоторые проблемы, связанные с ограничением

⁴¹² Обоснование данной позиции было приведено ранее в тексте данного параграфа (См. С. 148).

⁴¹³ См.: Приговор Ивановского районного суда Ивановской области №1-207/2010 по делу № 1-207/2010 в отношении Н.А. Кувакиной [Электронный ресурс]. URL: <http://sudact.ru/regular/doc/B3m6j7VeBj6i/> (дата обращения: 25.05.2016).

⁴¹⁴ См.: Приговор Ленинского районного суда г. Кирова № 1-586/2010 в отношении И.В. Михеева [Электронный ресурс]. URL: <https://rospravosudie.com/court-leninskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-100770808/> (дата обращения: 25.05.2016).

его от смежного состава, предусмотренного ст. 280 УК РФ («публичные призывы к осуществлению экстремистской деятельности»). По существу, проблема заключается в том, как соотносятся понятия «экстремизм» и «терроризм», «экстремистская» и «террористическая деятельность». Решение ее видится в следующем. В соответствии с положениями Федерального закона от 25.07.2002 № 114-ФЗ (ред от 06.07.2016) «О противодействии экстремистской деятельности» под экстремистской деятельностью понимается в том числе публичное оправдание терроризма и иная террористическая деятельность. Сравнительный анализ ст. 280 УК РФ с нормой, сформулированной в ст. 205² УК РФ, позволяет сделать вывод о том, что деяние в виде публичных призывов к осуществлению террористической деятельности выделено в самостоятельный состав преступления. Исследователи определяют соотношение данных норм как общая (ст. 280 УК РФ) и специальная (ст. 205² УК РФ): деяние, составляющее публичные призывы к осуществлению террористической деятельности, выделено в отдельную статью УК РФ⁴¹⁵. Есть основание полагать, что законодатель, предусматривая в УК РФ ст. 205² УК РФ, считает терроризм наиболее опасной формой проявления экстремизма. Об этом свидетельствует сравнительный анализ санкций в статьях 205² и 280 УК РФ: в ст. 205² УК РФ более строгая санкция⁴¹⁶.

Публичный призыв согласно содержанию Постановления Пленума ВС РФ от 09.02.2012 № 12 следует понимать как выраженные в любой форме обращения к другим лицам с целью побудить их к осуществлению террористической деятельности. Следует согласиться с формулировкой

⁴¹⁵ См.: Корнилов А.В. Разграничение публичных призывов к экстремистской и террористической деятельности // Вестник Томского государственного университета. 2013. № 4(10). С. 94.

⁴¹⁶ Федеральным законом от 28.12.2013 № 433-ФЗ была введена статья 280¹ УК РФ, устанавливающая ответственность за публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации. Данное общественно опасное деяние относится к экстремистской деятельности (экстремизму). См.: Чернявский Д.О., Скулаков Р.М. Публичные призывы к нарушению территориальной целостности: проблемы социально-политической обусловленности уголовно-правового запрета // Юридическая наука и правоохранительная практика. 2015. № 1(31). С. 76.

данного деяния и его толкованием в Постановлении Пленума Верховного суда РФ.

Между тем сегодня наблюдается возрастающая опасность изготовления, хранения и распространения материалов, которые призывают к осуществлению террористической деятельности или оправдывают ее. Террористическая пропаганда в сети Интернет в последнее время все больше тревожит специалистов в области противодействия различным проявлениям терроризма⁴¹⁷. Сущностное содержание такой пропаганды заключается в оказании воздействия, в том числе направленного на вербовку, иное подстрекательство, радикализацию общественных настроений и т.п.⁴¹⁸

Российское законодательство в сфере противодействия идеологии, составляющей основу терроризма, постоянно совершенствуется. Так, в 2015 году ст. 13.15 КоАП РФ была дополнена частью 6, устанавливающей ответственность в отношении юридических лиц за производство и выпуск продукции средств массовой информации, содержащей публичные призывы к осуществлению террористической деятельности, материалы, публично оправдывающие терроризм, и т.п.; была также усилена ответственность за производство и распространение экстремистских материалов (ст. 20.29. КоАП РФ)⁴¹⁹. Такая законодательная тенденция может быть признана положительной, однако представляется недостаточной.

Анализ уголовного законодательства некоторых бывших стран СНГ⁴²⁰, а также Великобритании (опыт которой довольно часто заимствуется

⁴¹⁷ См.: Сундиев И., Смирнов А. Сетевые возможности и сетевые угрозы: информационные сети в экстремистской и террористической деятельности // Свободная мысль–XXI. 2013. № 5. С. 195; Методические рекомендации по совершенствованию пропагандистской работы в сфере противодействия распространению идеологии терроризма в субъектах Российской Федерации / под общ. ред. В.В. Попова. М., 2013. С. 18. [Электронный ресурс]. URL: <http://www.dgu.ru/attachments/category/60/7.pdf> (дата обращения: 26.05.2016).

⁴¹⁸ См.: Использование Интернета в террористических целях // Управление Организации Объединенных Наций по наркотикам и преступности. Нью-Йорк, 2013. С. 4 [Электронный ресурс]. URL: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf (дата обращения: 26.05.2016).

⁴¹⁹ См.: Федеральный Закон от 02.05.2015 № 116-ФЗ «О внесении изменений в статьи 13.15 и 20.29 Кодекса Российской Федерации об административных правонарушениях» // СЗ РФ. 2015. № 18, ст. 2619.

⁴²⁰ Уголовный кодекс Республики Казахстан от 16 июня 1997 года в ч.1 ст. 233-1 устанавливает ответственность за пропаганду терроризма либо экстремизма или публичные призывы к совершению акта терроризма либо экстремизма, а равно распространение материалов указанного содержания. См.: Уголовный кодекс Республики Казахстан [Электронный ресурс]. URL:

Россией, несмотря на разницу в правовых системах) свидетельствует об определении ими в качестве преступных деяний, связанных с распространением (а равно с изготовлением и хранением в целях распространения) подобных материалов⁴²¹.

Российские исследователи также отмечают факт создания мощной медийной инфраструктуры, деятельность которой направлена на изготовление и распространение огромными тиражами материалов (видео-, аудио- и печатных), пропагандирующих идеологию, лежащую в основе деятельности террористической организации ИГИЛ, оправдывающих ее деятельность и призывающих к подражанию такой деятельности⁴²². Кроме того, в СМИ сообщалось, что после убийства Усамы бен Ладена были найдены жесткие диски и сотня флэш-накопителей с записями его посланий⁴²³.

В этой связи, говоря об общественной опасности изготовления, хранения и распространения материалов, оправдывающих террористическую деятельность или призывающих к ней, констатируем ее более высокую степень в сравнении с призывами и оправданием террористической деятельности, совершенными публично. Это тот скрытый террористический потенциал, который невозможно эффективно контролировать с помощью законодательства об административных правонарушениях.

Между тем считаем обоснованным расширить перечень действий, входящих в объективную сторону данного состава преступления (в отличие от составов, закрепленных в уголовном законодательстве Республики

http://online.zakon.kz/Document/?doc_id=31575252 (дата обращения: 15.05.2015); Уголовный Кодекс Украины в ч.1 ст. 258-2 устанавливает ответственность за публичные призывы к совершению террористического акта, а также распространение, изготовление или хранение с целью распространения материалов с такими призывами. См.: Уголовный кодекс Украины [Электронный ресурс]. URL: <http://meget.kiev.ua/kodeks/ugolovniy-kodeks/razdel-1-9/> (дата обращения: 15.05.2015).

⁴²¹ Уголовное право зарубежных стран. Общая и Особенная части: учебник для магистров / Н.А. Голованова, Е.В. Еремин, М.А. Игнатова [и др.]; под ред. Н.Е. Крыловой. 4-е изд., перераб. и доп. М.: Юрайт, 2013. С. 649.

⁴²² См.: Сундиев И.Ю., Смирнов А.А., Костин В. Н. Новое качество террористической пропаганды: медиа империя ИГИЛ [Электронный ресурс]. URL: <http://spkurdyumov.ru/biology/novoe-kachestvo-terroristicheskoy-propagandy-mediaiimperiya-igil/> (дата обращения: 15.11.2015).

⁴²³ См.: Козловский В. В США обнародованы материалы, изъятые у бин Ладена [Электронный ресурс]. URL: http://www.bbc.com/russian/international/2015/05/150521_osama_bin_laden_library (дата обращения 15.05.2016).

Казахстан и Украины), предусмотрев также ответственность за перевозку, ввоз на территорию Российской Федерации и вывоз с территории Российской Федерации таких материалов. Это обусловлено необходимостью максимально криминализовать все возможные действия по незаконному обороту указанных материалов, представляющих повышенную общественную опасность.

На основании изложенного предлагается следующая редакция ч. 1 ст. 205² УК РФ: публичное оправдание *террористической деятельности* либо публичные призывы к осуществлению террористической деятельности, *а равно распространение, изготовление, хранение, перевозка, ввоз на территорию Российской Федерации или вывоз с территории Российской Федерации в целях распространения материалов с такими призывами либо материалов, оправдывающих осуществление террористической деятельности*, - наказываются...

Рекомендованные изменения, связанные с определением сущности публичного оправдания в контексте ч. 1 ст. 205² УК РФ, требуют внесения изменений в Примечание 1 исследуемой статьи, которое необходимо изложить в следующей редакции: в настоящей статье под публичным оправданием *террористической деятельности* понимается *публичное признание террористической деятельности* правильной, нуждающейся в поддержке и подражании.

Последние изменения в УК РФ были в том числе связаны с включением Примечания 2 к ст. 205² УК РФ, разъясняющего сущность понятия террористическая деятельность, оценка которого приводилась ранее в настоящем диссертационном исследовании⁴²⁴. На основании проведенного анализа понятия «террористическая деятельность» и выводов о необходимости закрепления общеправового его значения на уровне Федерального закона РФ № 35-ФЗ, а также уголовно-правового – в Примечании 1.2 к ст. 205¹ УК РФ, Примечание 2 к ст. 205² УК РФ изложить

⁴²⁴ См.: Глава 1 § 1.

следующим образом. В настоящей статье под террористической деятельностью понимается совершение хотя бы одного из преступлений, предусмотренного статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, ст. 211 ч.4, 220, 221, 277, 278, 279, 360 и 361 настоящего Кодекса. Таким образом, из содержания понятия, предложенного законодателем, необходимо исключить ст. 205⁶ (диссертант полагает чрезмерной криминализацию данного состава⁴²⁵), ст. 206 (поскольку Указанием Генпрокуратуры России № 65/11 данное деяние относится к террористическим только при наличие в статистической карточке отметки о связи совершенного преступления с террористической деятельностью⁴²⁶), заменить ст. 211 на ч. 4 ст. 211 (поскольку Указанием Генпрокуратуры России № 65/11 только ч. 4 ст. 211 относится к деяниям террористической направленности).

Для целей эффективного применения исследуемой статьи под *материалами, содержащими публичные призывы к осуществлению террористической деятельности*, следует понимать любые носители информации (аудио-, видео-, печатные материалы), содержание которых направлено на побуждение других лиц к совершению хотя бы одного из преступлений, предусмотренных статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, 211 ч. 4, ст. 220, 221, 277, 278, 279, 360, 361 УК РФ.

Материалы, оправдывающие осуществление террористической деятельности, – любые носители информации (аудио-, видео-, печатные материалы), содержание которых направлено на признание террористической деятельности правильной, нуждающейся в поддержке и подражании.

Под *распространением* таких материалов следует понимать любые действия, направленные на отчуждение таких материалов, которые могут выражаться в следующем: продаже, безвозмездной передаче, дарении,

⁴²⁵ Правовая оценка данной статьи была дана в Главе 1 §1 настоящего диссертационного исследования.

⁴²⁶ Более того, ученые также склоняются к тому, что ст. 206 УК РФ нельзя признать безусловно преступлением террористической направленности. См.: Верина Г.В. Заведомо ложное сообщение об акте терроризма в редакции майского Федерального закон 2014 года // Библиотека криминалиста. Научный журнал. 2014. № 6 (17). С. 19-20.

предоставлении займы, предложении таких материалов для продажи или займы, предоставлении другим лицам услуги в виде возможности получить, прочитать, услышать или посмотреть такие материалы и т.п.

Под *изготовлением* таких материалов следует понимать совершение любых действий, направленных на создание таких материалов: запись видео-призывов на компакт-диски, печать брошюр, листовок, книг, содержание которых направлено на признание террористической деятельности правильной, нуждающейся в поддержке и подражании либо на призыв к осуществлению террористической деятельности, если они совершены в целях их распространения.

Под *хранением* в контексте ч. 1 ст. 205² УК РФ следует понимать владение такими материалами с целью дальнейшего их распространения.

Перевозка указанных материалов означает их транспортировку любым транспортным средством в целях их распространения.

Ввоз на территорию Российской Федерации и вывоз с территории Российской Федерации – предполагает перемещение любым способом на территорию Российской Федерации либо за пределы территории Российской Федерации материалов призывающих или оправдывающих террористическую деятельность в целях их распространения.

Следует также отметить, что призывы или оправдание террористической деятельности должны быть совершены публично. На сегодняшний день вопрос о публичности призывов и оправдания согласно п. 19 Постановления Пленума ВС РФ от 09.02.2012 № 12, разрешается судами с учетом места, способа, обстановки и других обстоятельств дела; в том числе публичным признается совершение указанных действий в информационно-телекоммуникационных сетях общего пользования, включая сеть Интернет, например, на сайтах, форумах или в блогах, распространение обращений путем массовой рассылки электронных сообщений и т.п.

Использование информационно-телекоммуникационных сетей (в том числе сети Интернет) является квалифицирующим или особо

квалифицирующим признаком некоторых составов преступлений, предусмотренных УК РФ.

Российское законодательство последние несколько лет стоит на пути реформирования в связи с активным внедрением информационных технологий во все сферы жизни общества. На сегодняшний день исследователи различных проблем уголовно-правовой науки настаивают на необходимости дальнейшего совершенствования уголовного законодательства в части внесения изменений и дополнений в статьи предусматривающие ответственность за незаконный оборот наркотических средств и психотропных веществ, совершение развратных действий и др., связанных с включением квалифицирующего или особо квалифицирующего признака: «использование информационно-телекоммуникационных сетей, в том числе сети Интернет»⁴²⁷.

Отсутствие правового регулирования национальных электронных ресурсов, международных правовых соглашений, связанных с правовым регулированием всего киберпространства, создает проблемы, связанные с противодействием терроризму, экстремизму, распространением порнографии. Ранее в рамках настоящей работы были рассмотрены признаки, характеризующие общественную опасность информационного терроризма, к которым, в том числе, относится анонимность, дешевизна ресурсов, стремительные процессы информатизации (за 2014 год число россиян старше 16 лет, пользующихся Интернетом, увеличилось более чем на 10 % по сравнению с предыдущим годом)⁴²⁸. В своем докладе первый заместитель руководителя аппарата НАК Е.П. Ильин отмечал, что одной из основных установок в работе по направлению противодействия идеологии, составляющей основу терроризма, является понимание того, что наибольшие

⁴²⁷ См.: Тасаков С.В. Развратные действия в сети Интернет // Уголовное право. 2014. № 5. С. 97.

⁴²⁸ См.: Пользование Интернетом в России: итоги 2014 года [Электронный ресурс]. URL: https://www.gfk.com/fileadmin/user_upload/dyna_content/RU/Documents/News/2015/Internet_in_Russia_2014-final_full.pdf (дата обращения: 16.11.2015)

угрозы ее распространения связаны с использованием террористическими и экстремистскими организациями сети Интернет⁴²⁹.

Изменения, связанные с включением нового квалифицирующего признака, коснулись и ст. 280 УК РФ, предусматривающей ответственность за публичные призывы к осуществлению экстремистской деятельности. Федеральным законом от 28.06.2014 году № 179-ФЗ в ч. 2 ст. 280 УК РФ были внесены изменения, связанные с выделением еще одного квалифицирующего признака⁴³⁰, наравне с средствами массовой информации, такого как совершение преступления, указанного в ч. 1 ст. 280 УК РФ, с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет.

На это несоответствие обратил внимание в том числе и законодатель. В связи с последними изменениями в УК РФ диспозиция ч. 2 ст. 205² УК РФ была дополнена и изложена в следующей редакции: «те же деяния, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет».

Определенные сомнения вызывает указание на электронные сети. Анализ УК РФ показывает, что в диспозициях ч. 1 ст. 185³ («манипулирование рынком»), ч. 2 ст. 280¹ («публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации») и ч. 2 п. «б» ст. 228¹ («незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконный сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества»)

⁴²⁹ См.: Доклад первого заместителя руководителя аппарата НАК Ильина Е.П. // Материалы III-й Всероссийской научно-практической конференции «Концепция противодействия терроризма в РФ. Комплексный подход к формированию и функционированию системы противодействия распространения идеологии терроризма». Т. 1. М., 2012. С. 8 [Электронный ресурс]. URL: http://www.dagminobr.ru/storage/files/protivodeistvie%20terrorizmu/mat_vseros_konf_tom1.pdf (дата обращения: 28.05.2016).

⁴³⁰ См.: Федеральный Закон от 28.06.2014. № 179-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2014. № 26 (ч. I), ст. 3385.

предусматривается данное понятие наравне с информационно-телекоммуникационной сетью, в том числе сетью Интернет. Причем техника построения данного квалифицирующего (или особо квалифицирующего) признака свидетельствует о том, что электронная сеть – это сеть, отличная, несовпадающая, иными словами – другая сеть.

Между тем диспозиции ч. 1 ст. 171² («незаконные организация и проведения азартных игр»), ч. 3 п. «б» ст. 242 («незаконные изготовление и оборот порнографических материалов и предметов»), ч. 2 п. «г» ст. 242¹ («изготовление и оборот материалов или предметов с порнографическим изображением несовершеннолетних»), ч. 2 п. «г» ст. 242² («использование несовершеннолетнего в целях изготовления порнографических материалов или предметов»), ч. 2 ст. 280 («публичные призывы к осуществлению экстремистской деятельности») и ч. 1 ст. 282 («возбуждение ненависти либо вражды, а равно унижение человеческого достоинства») УК РФ предусматривают квалифицирующий (или особо квалифицирующий) признак, связанный с использованием информационно-телекоммуникационной сети, в том числе сети Интернет.

Такая законодательная неопределенность и отсутствие единства в формулировке исследуемого признака могут быть обусловлены лишь особенностью (спецификой) электронной сети. Однако положения Федерального закона РФ от 27.07.2006 № 149-ФЗ (ред. от 06.07.2016) «Об информации, информационных технологиях и о защите информации» не содержат понятия электронной сети, разъясняя лишь понятия «электронное сообщение» и «электронный документ». Сущность последних, в свою очередь, раскрывается через понятие информационно-телекоммуникационной сети⁴³¹.

⁴³¹ Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети; электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Кроме того, как отмечает И.М. Рассолов, существовавшее ранее деление на типы сетей, различавшихся по их функциональной принадлежности (кабель для передачи аудиовизуальных, телефонных и иных данных), теряют актуальность сегодня под воздействием технологической конвергенции (слияния)⁴³². Все типы сетей объединены понятием «информационно-телекоммуникационная сеть».

Сказанное свидетельствует о том, что указание в исследуемом квалифицирующем (или особо квалифицирующем) признаке на электронную сеть чрезмерно, поскольку данная сеть является типом информационно-телекоммуникационной сети. С целью избежания двусмысленности в определении признаков составов преступлений необходимо исключить понятие «электронная сеть» из диспозиций ч. 1 ст. 185³, ч. 2 ст. 280¹, ч. 2 п. «б» ст. 228¹ УК РФ.

На основании изложенного, ч. 2 ст. 205² УК РФ изложить в следующей редакции: те же деяния, совершенные с использованием СМИ *либо информационно-телекоммуникационных сетей, в том числе сети Интернет,* - наказываются...

В заключение следует отметить, что уголовно-правовые меры противодействия информационному терроризму должны осуществляться в двух направлениях, соответствующих видам исследуемого явления: информационно-технологическом и информационно-психологическом.

Информационно-технологическое направление противодействия информационному терроризму включает в себя:

1) совершенствование нормы, устанавливающей ответственность за террористический акт (ст. 205 УК РФ), в части изменения целей. На основе проведенного анализа диссертант полагает, что предусмотренные в ч. 1 ст. 205 УК РФ цели террористического акта не отражают сущность совершаемых деяний и не позволяют решить проблемы квалификации.

⁴³² См.: Рассолов И.П. Право и Интернет. Теоретические проблемы. 2-е изд., доп. М.: Норма, 2009. 384 с. [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

2) внесение изменений в ст. 205 УК РФ для целей обеспечения безопасности автоматизированных систем управления критически важных объектов и потенциально опасных объектов от террористических угроз.

3) признание деяний, предусмотренных статьями 272 и 273 УК РФ равными по степени и характеру общественной опасности, в связи с чем изложить квалифицированные признаки ст. 273 УК РФ по аналогии со ст. 272 УК РФ и предусмотреть максимальное наказание по ч. 1 – до двух лет лишения свободы, по ч. 2 – до четырех лет лишения свободы, по ч. 3 – до семи лет лишения свободы.

4) внесение изменений в ч. 2 ст. 272 и ч. 2 ст. 273 УК РФ, в части установления квалифицирующего признака: «с целью скрыть другое преступление или облегчить его совершение».

Информационно-психологическое направление противодействия информационному терроризму включает в себя:

1) совершенствование ст. 205² УК РФ, что обусловлено проблемами в квалификации совершаемых деяний; а также дополнение ч. 1 ст. 205 УК РФ такими альтернативными деяниями, как «распространение, изготовление, хранение, перевозка, ввоз на территорию Российской Федерации или вывоз с территории Российской Федерации в целях распространения материалов с такими призывами либо материалов, оправдывающих осуществление террористической деятельности», что обусловлено возрастающей опасностью террористической пропаганды.

2) изменение содержания квалифицирующего признака ч. 2 ст. 205² УК РФ, что обусловлено необходимостью точного и недвусмысленного содержания норм Особенной части УК РФ.

3) совершенствование примечания к ст. 205² УК РФ, необходимость которого обусловлено теми изменениями, которым подвергается часть 1 исследуемой статьи.

§2 Иные меры противодействия информационному терроризму

На сегодняшний день не существует единой точки зрения по вопросу определения правильных, достаточных и эффективных мер противодействия преступности в целом и терроризму в частности. Российская политика в сфере противодействия терроризму имеет большой опыт, о чем свидетельствует значительное количество правовых актов, регламентирующих вопросы предупреждения, профилактики терроризма и борьбы с ним, и история их изменений. Как отмечает Н.А. Лопашенко, на сегодняшний день ни ученые, ни практики, ни общество, ни законодатель не знают надежных критериев эффективности политики противодействия терроризму: должна ли она соответствовать общему направлению гуманизации уголовной политики либо быть более жесткой, что оправдывается повышенной общественной опасностью явления терроризма⁴³³.

Так, некоторые исследователи определяют в качестве эффективных меры по усилению ответственности за террористические акты и иные преступления террористической направленности⁴³⁴; другие делают акцент на необходимости выявления и устранения причин и условий терроризма, к которым относят экономическую нестабильность, низкий уровень жизни, межэтнические, межконфессиональные и иные социальные противоречия и т.п.⁴³⁵. Так или иначе ученым, законодателям и правоприменителям следует уделять внимание всем возможным мерам противодействия терроризму.

Противодействие терроризму составляет систему комплексных мер по профилактике, предупреждению терроризма, пресечению преступлений (правонарушений) террористической направленности, а также привлечению

⁴³³ См.: Лопашенко Н.А. Уголовная политика. М.: Волтерс Клувер, 2009. С. 380.

⁴³⁴ См.: Попов В.Г. О концепции государственного управления и регулирования противодействия терроризму // Борьба с терроризмом: актуальные проблемы законодательного обеспечения: сб. науч. ст. Ростов н/Д: РЮИ МВД России, 2003. С. 84-89; Алехнович С.О. Терроризм и антитерроризм: актуальный ракурс // Российский следователь. 2007. № 3. С. 26-27.

⁴³⁵ См.: Кудрявцев В.Н. Терроризм и организованная преступность в условиях глобализации мира // Борьба с терроризмом: сб. / сост. Л.В. Брятова; науч. ред. В.Н. Кудрявцев. М.: Наука, 2004. С. 5-80.

виновных лиц к ответственности и устранению (уменьшению) последствий таких преступлений (правонарушений) и т.п..

На сегодняшний день проектом Конвенции об обеспечении международной информационной безопасности предложены основные меры противодействия использованию информационного пространства в террористических целях. Данные меры связаны с установлением международного сотрудничества по вопросам такого противодействия, проведением следственных, розыскных и процессуальных мероприятий, направленных на предотвращение, пресечение и ликвидацию последствий проведения террористических действий в информационном пространстве, а также наказание виновных в них лиц и организаций. Однако названные меры носят общерекомендательный характер и не учитывают особенностей российской законодательной и организационной системы противодействия терроризму.

По нашему мнению, система мер противодействия информационному терроризму должна основываться на комплексе существующих мер противодействия терроризму, разработанному в законодательстве и доктрине.

С целью систематизации следует различать следующие меры противодействия терроризму, на основе которых требуется конкретизировать особенности противодействия информационному терроризму:

- 1) общеправовые превентивные меры противодействия терроризму;
- 2) специализированные меры противодействия терроризму (уголовно-правовые, административно-правовые);
- 3) организационные – разработку и повышение эффективности организационных основ противодействия терроризму;
- 4) пресечение совершения преступлений (правонарушений) террористической направленности, а также устранение (уменьшение) последствий таких преступлений (правонарушений);

5) повышение уровня внутренней безопасности учреждений и организаций

6) международное сотрудничество в сфере противодействия терроризму;

7) иные меры, связанные с повышением уровня правосознания и правовой культуры населения Российской Федерации.

Следует заметить, что на современном этапе развития российской уголовной политики приоритет отдается профилактическим и предупредительным мерам противодействия терроризму⁴³⁶. К превентивным задачам такого противодействия Концепцией были отнесены:

1) выявление и устранение причин и условий терроризма;

2) выявление, предупреждение и пресечение действий лиц и организаций, направленных на подготовку и совершение террористических актов и иных преступлений террористического характера;

3) поддержание в состоянии постоянной готовности к эффективному использованию сил и средств, предназначенных для выявления, предупреждения террористической деятельности;

4) обеспечение безопасности граждан и антитеррористической защищенности потенциальных объектов террористических посягательств, в том числе критически важных объектов инфраструктуры и жизнеобеспечения;

5) противодействие распространению идеологии терроризма и активизация работы по информационно-пропагандистскому обеспечению антитеррористических мероприятий⁴³⁷.

Помимо названных, к основным задачам противодействия терроризму отнесены также меры:

⁴³⁶ См.: Концепция противодействия терроризму в Российской Федерации (утв. Президентом 5 октября 2009 года) // Рос. газета. 2009. 20 окт.

⁴³⁷ См.: Там же.

- по выявлению, предупреждению и пресечению действий лиц и организаций, направленных на подготовку и совершение террористических актов и иных преступлений террористического характера⁴³⁸;
- по привлечению к ответственности субъектов террористической деятельности в соответствии с законодательством РФ.

Общеправовые превентивные меры противодействия терроризму связаны в первую очередь с разработкой и совершенствованием общеправового законодательства. К таковому на сегодняшний день следует относить Конституцию РФ, Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму», иные правовые акты, регламентирующие вопросы, связанные с обращением оружия, обеспечением безопасности, а также Концепцию противодействия терроризму в Российской Федерации.

Фундаментальным значением в эффективном противодействии любому негативному явлению (коррупции, терроризму, экстремизму и т.п.) обладает точная законодательная регламентация сущности и содержания используемого понятийного аппарата. В связи с предложенными в рамках данного диссертационного исследования трактовками понимания терроризма, террористической деятельности и преступлений (правонарушений) террористической направленности необходимо внести изменения в Федеральный закон РФ от 06.03.2006 № 35-ФЗ «О противодействии терроризму» в указанной части.

Кроме того, с учетом специфики изучаемого в рамках данного диссертационного исследования явления, помимо мер, направленных на противодействие любым возможным формам и видам терроризма,

⁴³⁸ За 2015 год правоохранительными органами было предотвращено 30 преступлений террористической направленности. Но несмотря на то, что Национальный антитеррористический комитет весьма положительно оценивает работу правоохранительных органов в этой сфере, А.В. Бортников в своем выступлении озвучил важнейшие направления деятельности всех силовых и иных структур по противодействию терроризму и всем террористическим проявлениям. См.: Выступление председателя национального антитеррористического комитета, директора ФСБ России А.В. Бортникова на открытии совместного заседания НАК и ФОШ. Москва, 15.12.2015 [Электронный ресурс]. URL: <http://nac.gov.ru/publikacii/vystupleniya-i-intervyu/vystuplenie-predsedatelya-nacionalnogo-0.html> (дата обращения: 08.07.2016).

необходимо разрабатывать и иные, направленные на эффективное предотвращение и предупреждение информационного терроризма.

Информационный терроризм как уникальная форма терроризма характеризуется осуществлением террористической деятельности на платформе информационного пространства. В связи с этим особое внимание следует уделять обеспечению безопасности информационной сферы (иначе – информационной безопасности). На сегодняшний день существует несколько документов, принятых за последнее время Российской Федерацией, частично затрагивающих вопросы противодействия возможным угрозам в информационном пространстве: Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации⁴³⁹, Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации⁴⁴⁰, Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года⁴⁴¹, Доктрина информационной безопасности Российской Федерации⁴⁴², Проект конвенции об обеспечении международной информационной безопасности (концепция)⁴⁴³.

⁴³⁹ См.: Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (Концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

⁴⁴⁰ См.: Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

⁴⁴¹ См.: Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом Российской Федерации В. Путиным 24 июля 2013 года, № Пр-1753) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

⁴⁴² См.: Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации В. Путиным 9 сентября 2000 г. № Пр-1895) // Рос. газета. 2000. 28 сент.

⁴⁴³ См.: Проект конвенции об обеспечении международной информационной безопасности (концепция) [Электронный ресурс]. URL: <http://www.scrf.gov.ru/documents/6/112.html> (дата обращения: 07.11.2015).

Все названные выше документы не лишены положительных моментов при определении мер по обеспечению информационной, компьютерной безопасности, безопасности автоматизированных систем управления. Однако ни один из них не имеет определенного юридического статуса, а положения, содержащиеся в них, не нашли своего отражения в системе российского законодательства.

Безусловно, разработка концепций или основных направлений противодействия какому-либо масштабному явлению, например коррупции, терроризму, организованной преступности, имеет положительные тенденции. Многие зарубежные страны уже давно приняли общеправовые документы (стратегии, концепции), содержащие положения об обеспечении безопасности информационного и киберпространств от возможных угроз, в их числе – Канада, США, Германия, Республика Корея, Китай, Франция, Израиль, Великобритания, Пакистан и др.⁴⁴⁴ Разработка таких концепций или стратегий является первым этапом на пути формирования национального законодательства в сфере обеспечения информационной безопасности. Однако Российская Федерация слишком долго задерживается на данном этапе.

В первую очередь необходимо разработать Стратегию по обеспечению информационной безопасности Российской Федерации на основе Проекта конвенции об обеспечении международной информационной безопасности (концепции) с некоторыми изменениями в части:

1) понятийно-категориального аппарата (в частности, таких как «информационное пространство», «информационные ресурсы», «терроризм в информационном пространстве»⁴⁴⁵). Понятия информационного пространства и информационной безопасности являются базовыми,

⁴⁴⁴ См.: Ковлагина Д.А. Анализ кибернетического потенциала зарубежных стран // Право: теория и практика. 2013. № 11. С. 50-53.

⁴⁴⁵ Проблемы формирования понятийного аппарата не раз обсуждались многими исследователями. См.: Демидов О. Обеспечение международной информационной безопасности и Российские национальные интересы. С. 137 [Электронный ресурс]. URL: <http://www.pircenter.org/media/content/files/10/13559089230.pdf> (дата обращения: 18.06.2015).

фундаментальными для разработки эффективных мер противодействия терроризму и иным противоправным посягательствам в данной сфере;

2) определения основных угроз информационной безопасности;

3) определения мер противодействия использованию информационного пространства террористами, террористическими организациями (или сообществами).

Кроме того, необходимо внести некоторые изменения в Федеральный закон РФ № 149-ФЗ «Об информации, информационных технологиях и защите информации» в части:

- раскрытия сущности и содержания таких понятий, как «информационное пространство», «информационные ресурсы», «информационная безопасность». Также должно быть конкретизировано понятие информационных технологий. Такая мера является необходимой в связи с возможностью определения данных явлений в качестве средств («орудий»), предметов, платформы преступных посягательств и правонарушений в информационной сфере.

Безусловно, основное внимание необходимо уделять профилактическим и предупредительным мерам противодействия самым масштабным и опасным явлениям, сопровождающим общественное развитие, – экстремизму, терроризму, организованной преступности и т.д. Исследователи в области обеспечения информационной безопасности отмечают необходимость формирования комплекса превентивных мер от возможных угроз в информационном пространстве⁴⁴⁶. Однако в случае невозможности своевременного предотвращения проявлений какого-либо общественно опасного явления возникает необходимость в разработке и дальнейшем усовершенствовании специальных мер. К таковым следует относить, в частности, уголовно-правовые меры. В рамках данного

⁴⁴⁶ См.: Алиева М.Ф. Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2012. № 4. С. 101.

диссертационного исследования названные меры уже подверглись детальному рассмотрению в отдельном параграфе.

Наравне с общеправовыми мерами противодействия терроризму особое значение имеют *меры, связанные с разработкой и повышением эффективности организационных основ противодействия терроризму*. Данные меры связаны с определением роли, полномочий и обязанностей государственных органов, органов власти субъектов РФ, правоохранительных органов, специализированных структур (например, национального антитеррористического комитета) в сфере противодействия терроризму, а также повышением профессионального уровня сотрудников названных органов и структур⁴⁴⁷.

В отношении *информационного терроризма* данные меры должны сопровождаться также активной совместной работой органов и структур, названных выше, с Управлением «К» МВД России, иными специализированными подразделениями, связанными с обеспечением безопасности информационно-телекоммуникационных сетей. Кроме того, необходимо разработать условия сотрудничества органов и структур, задачей которых является противодействие терроризму и всем террористическим проявлениям, с негосударственными учреждениями и организациями, деятельность которых связана с обеспечением внутренней информационной безопасности. В настоящее время существует достаточное количество таких организаций, направленных в том числе на оказание помощи частному сектору, правоохранительным органам в вопросах внутренней информационной безопасности. Самая известная такая организация – USRAND – corporation по заказам правительства США проводит

⁴⁴⁷ Например, Р.И. Дремлюга предлагает создать единую структуру, контролирующую деятельность и распространение информации в сети Интернет. См.: Дремлюга Р.И. Интернет-преступность: дис. ... канд. юрид. наук. Владивосток, 2007. С. 214; За 2015 год проводилась работа по повышению квалификации 12 тысяч работников образования, сотрудников правоохранительных органов, государственных и муниципальных служащих в сфере противодействия терроризму. См.: Выступление председателя национального антитеррористического комитета, директора ФСБ России А.В. Бортникова на открытии совместного заседания НАК и ФОШ. Москва, 15.12.2015 [Электронный ресурс]. URL: <http://nac.gov.ru/publikacii/vystupleniya-i-intervyu/vystuplenie-predsedatelya-nacionalnogo-0.html> (дата обращения: 08.07.2016).

исследования в области национальной безопасности. В Российской Федерации известна такая международная компания, как GroupIB, деятельность которой связана с предотвращением и расследованием киберпреступлений и мошенничеств с использованием высоких технологий. GroupIB оказывает помощь частному сектору, а также правоохранительным органам в расследовании компьютерных преступлений.⁴⁴⁸

В силу возрастающей угрозы информационного воздействия, которая может иметь как опосредованный, так и непосредственный характер, остается актуальной проблема мониторинга СМИ на предмет выявления материалов с экстремистским и террористическим контентом⁴⁴⁹. Для целей предупреждения негативного воздействия на население следует разработать условия сотрудничества специализированных структур с негосударственными организациями саморегулирования СМИ по вопросу выявления публикаций, возбуждающих ненависть или вражду в отношении каких-либо социальных групп, а также публикаций, оказывающих поддержку террористической деятельности или оправдывающих её, и т.п.

Особая роль в противодействии терроризму отводится правоохранительным, правоприменительным органам, а также иным специализированным структурам, деятельность которых направлена на **выявление и пресечение преступлений (правонарушений) террористической направленности, а также устранение (уменьшение) последствий таких преступлений (правонарушений)**. Такая деятельность может быть связана с получением информации о местонахождении террористических и экстремистских организаций; проведением различных оперативно-розыскных мероприятий; взаимодействием правоохранительных органов и специализированных структур РФ и иностранных государств по

⁴⁴⁸ См.: Одна из ведущих компаний в мире по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий [Электронный ресурс]. URL: <http://www.group-ib.ru> (дата обращения 09.04.2015).

⁴⁴⁹ См.: Методические рекомендации по совершенствованию пропагандистской работы в сфере противодействия распространению идеологии терроризма в субъектах Российской Федерации / под ред. В.В. Попова. М., 2013. С. 15 [Электронный ресурс]. <http://scienceport.ru/files/metod2013.pdf> (дата обращения: 17.11.2015).

выявлению и пресечению преступлений (правонарушений) террористической направленности⁴⁵⁰, привлечению виновных лиц к ответственности и т.п.

Кроме того, одной из важнейших задач противодействия угрозам в информационном пространстве (в частности, угрозы *информационного терроризма*, информационной войны и информационных преступлений) является развитие и совершенствование кадрового обеспечения информационной безопасности⁴⁵¹. В этой связи полезен опыт зарубежных стран, таких как Великобритания, КНДР, КНР, Иран и другие⁴⁵², сформировавших за последние несколько лет специализированные кибернетические подразделения, деятельность которых направлена на предотвращение возможных угроз в киберпространстве⁴⁵³.

Необходимо также обратить внимание на вопросы процедуры распознавания и блокировки, возможно с помощью мониторинга, осуществляемого общественными организациями и объединениями, веб-сайтов, размещающих информацию о деятельности террористических групп (организаций, сообществ), пропагандирующих идеологию, присущую терроризму и экстремизму, а также направленных на вовлечение в террористическую деятельность⁴⁵⁴.

Немаловажным в системе мер противодействия терроризму является ***обеспечение внутренней безопасности учреждений и организаций***, в

⁴⁵⁰ См.: Аккаева Х.А. Характеристика терроризма в современной России и основные направления деятельности органов внутренних дел по борьбе с данным социально опасным явлением // Теория и практика общественного развития. 2014. № 2. С. 419-421.

⁴⁵¹ См.: Бурькова Е.В. Профессиональная подготовка специалистов в области информационной безопасности // Вестник Оренбургского государственного университета. 2016. № 2(190). С. 3.

⁴⁵² Например, иранское кибернетическое подразделение на 2010 год составляло 2400 человек, разрабатывающих способы, методы взлома программного обеспечения любой степени защищенности, создания помех, компьютерных вирусов, компьютерной и сетевой разведки и т.п.

⁴⁵³ См.: Siavash «Iranian Cyber Warfare Threat Assessment» [Электронный ресурс]. URL: <http://www.cyberwarzone.com/content/iranian-cyber-warfare-threat-assessment> (дата обращения: 27.05.2016).

⁴⁵⁴ В первом полугодии 2015 было заблокировано более 3 тысяч информационных ресурсов, пропагандирующих идеологию, присущую терроризма. См.: Выступление председателя национального антитеррористического комитета, директора ФСБ России А.В. Бортникова на открытии совместного заседания НАК и ФОШ. Москва, 15.12.2015 [Электронный ресурс]. URL: <http://nac.gov.ru/publikacii/vystupleniya-i-intervyu/vystuplenie-predsedatelya-nacionalnogo-0.html> (дата обращения: 08.07.2016).

особенности критически важных и потенциально опасных объектов Российской Федерации⁴⁵⁵.

На сегодняшний день крупные организации и учреждения активнее внедряют системы автоматизированного управления, что, безусловно, облегчает работу производств, но и не лишено определенных рисков. Сдерживающим и положительным фактором, способствующим предупреждению *информационного терроризма*, является совершенствование системы внутренней информационной защиты от возможных посягательств с помощью сети Интернет или иной локальной сети (включая обучение сотрудников таких организаций по вопросу обеспечения информационной безопасности непосредственно на рабочих местах), а также принятию эффективных мер по защите информации от ее незаконного использования⁴⁵⁶.

Терроризм представляет собой одну из самых масштабных угроз сегодняшней действительности, требующих всеобщей мобилизации государств в противодействии этому явлению. Возрастающая опасность терроризма определяется возникшей угрозой использования террористами (террористическими организациями, сообществами) информационного пространства (характеризующегося невозможностью установления географических или геополитических границ). Это обуславливает необходимость *установления и укрепления международного сотрудничества государств по вопросу обеспечения информационной безопасности, в том числе от террористических угроз*. В первую очередь такое сотрудничество должно выражаться в формировании на

⁴⁵⁵ См.: Поручение Президента РФ от 15.11.2011 г. № Пр-3400 «Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года» [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

⁴⁵⁶ См.: Боровский А.С. Модели, методы и алгоритмы интеллектуальной поддержки принятия решений в задачах разработки и оценки систем физической защиты объектов информатизации: автореф. дис. ... д-ра технич. наук. СПб., 2015. С. 7-9; Дремлюга Р.И. Указ. соч. С. 215-220.

международном уровне понятия информационного терроризма⁴⁵⁷, которое могло бы выступить основой для совершенствования национального законодательства государств в сфере обеспечения информационной безопасности.

Кроме того, Российская Федерация должна стать постоянным участником и организатором проводимых кибернетических учений. Такие государства, как Швеция, Франция, Сингапур, повышают свой кибернетический потенциал за счет организации или участия в кибернетических упражнениях. Так, Швеция в мае 2010 года участвовала в международных упражнениях «Балтийский Кибер Щит», которые были организованы Эстонией (при поддержке НАТО). Кроме того, Швеция является членом оборонного упражнения, имитирующего нападение террористов и враждебных государств на критически важные инфраструктуры⁴⁵⁸.

Администрация Сингапура совместно с созданным в 2009 г. Управлением по защите информационно-коммуникационных технологий проводила игры и упражнения для укрепления кибербезопасности страны⁴⁵⁹.

Такие упражнения направлены на обмен опытом в противодействии террористическим угрозам в киберпространстве, являющемся частью пространства информационного⁴⁶⁰.

⁴⁵⁷ В Докладе Генерального секретаря ООН было изложено понятие информационного терроризма, анализ которого не позволяет определить его существенные признаки / Доклад Генерального секретаря ООН: A/55/140/Генеральная Ассамблея ООН: Пятьдесят пятая сессия. 2000. 10 июля.

⁴⁵⁸ См.: Sweden has central role in cyber warfare [Электронный ресурс]. URL: <http://www.dn.se/nyheter/sverige/sweden-has-central-role-in-cyber-warfare> (дата обращения: 13.04.2016).

⁴⁵⁹ См.: Dawn Tay «Govt sets up cyber-security agency» [Электронный ресурс]. URL: <http://www.asiaone.com/News/AsiaOne+News/Singapore/Story/A1Story20091001-171044.html> (дата обращения: 13.04.2016).

⁴⁶⁰ В октябре 2015 года прошли третьи Европейские учения по кибербезопасности среди 27 стран: Бельгия, Чехия, Германия, Эстония, Греция, Великобритания, Испания, Франция, Италия, Латвия, Литва, Ирландия, Венгрия, Нидерланды, Польша, Португалия, Румыния, Словения, Финляндия, Швеция, Австрия, Кипр, Люксембург, Норвегия, Исландия, Хорватия и Турция. Организаторами данного мероприятия выступили ENISA (Европейское агентство по безопасности сетей и информационной безопасности), Европейская комиссия и более 100 партнеров, среди которых региональные органы власти, университеты, научно-исследовательские центры и т.п. Российская Федерация не принимала участия в данном мероприятии. См.: Деятельность ENISA за октябрь 2015 [Электронный ресурс]. URL: <http://d-russia.ru/devyatnost-enisa-za-oktyabr-2015-goda.html> (дата обращения: 08.07.2016).

Предложенные меры противодействия информационному терроризму не смогут в полной мере обеспечить необходимую защиту без особого направления деятельности, связанного с предотвращением причин и условий терроризма независимо от его видов и форм. В.Е. Петрищев обоснованно отмечает необходимость ведения грамотной национальной, культурной политики, повышения уровня правового сознания населения, контрпропаганды идеологий терроризма и экстремизма⁴⁶¹. Данное направление стало одним из ведущих, избранным на 2016 год Национальным антитеррористическим комитетом, в условиях сохраняющейся тенденции к росту количества радикально настроенных лиц⁴⁶². В первую очередь оно должно проявляться в формировании у населения (в особенности подростковых групп и молодежи) устойчивого негативного отношения ко всем возможным проявлениям терроризма, насилия, нетерпимости и т.п.

Таким образом, система мер противодействия информационному терроризму должна включать в первую очередь общепреventивные и профилактические меры, к которым следует относить:

- разработку и совершенствование специализированного понятийного аппарата в сфере обеспечения информационной безопасности путем принятия и внесения изменений в правовые акты, регламентирующие вопросы защиты информации и правомерного использования информационных технологий;

- повышение эффективности сотрудничества органов и структур, направление деятельности которых связано с противодействием терроризму, с Управлением «К» МВД России, иными специализированными подразделениями, связанными с обеспечением безопасности

⁴⁶¹ См.: Петрищев В.Е. Противодействие террористической идеологии – приоритетное направление профилактики терроризма // II Всероссийская научно-практическая Конференция в МГУ им. М.В. Ломоносова. Москва, 2010 [Электронный ресурс]. URL: <http://nac.gov.ru/publikacii/stati-knigi-broshyury/petrishchev-ve-protivodeystvie.html> (дата обращения: 09.11.2015).

⁴⁶² См.: Выступление председателя национального антитеррористического комитета, директора ФСБ России А.В. Бортникова на открытии совместного заседания НАК и ФОШ. Москва, 15.12.2015 [Электронный ресурс]. URL: <http://nac.gov.ru/publikacii/vystupleniya-i-intervyu/vystuplenie-predsedatelya-nacionalnogo-0.html> (дата обращения: 08.07.2016).

информационно-телекоммуникационных сетей, а также с негосударственными учреждениями и организациями, деятельность которых связана с обеспечением внутренней информационной безопасности;

- разработку условий сотрудничества специализированных структур с негосударственными организациями саморегулирования СМИ по вопросу выявления публикаций, возбуждающих ненависть или вражду в отношении каких-либо социальных групп, а также публикаций, оказывающих поддержку или оправдывающих террористическую деятельность, и т.п.;

- развитие и совершенствование кадрового обеспечения информационной безопасности;

- совершенствование системы внутренней информационной защиты учреждений и организаций от возможных посягательств с помощью сети Интернет (иной локальной или территориальной сети), а также иных информационных технологий;

- установление и укрепление международного сотрудничества государств в сфере обеспечения информационной безопасности от возможных угроз террористического характера;

- иные меры превентивного характера, связанные с формированием у населения негативного отношения ко всем возможным проявлениям терроризма, к использованию насилия для достижения целей терроризма, ксенофобии и экстремизму.

ЗАКЛЮЧЕНИЕ

На основании проведенного исследования определения сущности, уголовно-правовых и иных мер противодействия информационному терроризму можно сформулировать следующие выводы.

Несмотря на то что явление терроризма сопровождает человечество на протяжении более чем 200 лет, на международном уровне до сих не разработано соответствующей дефиниции.

Следует сказать, что единого подхода к пониманию сущности терроризма и его признаков не выработано и в российском законодательстве и доктрине. Многие исследователи определяют терроризм как совершение действий или применение насилия, другие характеризуют его как социальное, социально-правовое, социально-политическое явление.

В результате проведенного анализа имеющихся подходов к пониманию терроризма и его признаков, а также истории исследуемого понятия, диссертант определил в качестве сущностных следующие признаки терроризма: терроризм представляет собой практику воздействия; воздействие является идеологически обоснованным; кроме того, оно сопряжено с устрашением населения; воздействие имеет опосредованный характер (имущественный, физический и иной вред причиняется одним лицам (тактические объекты), а воздействие осуществляется на других (стратегические объекты)).

Выделенные признаки способствовали формированию авторской дефиниции терроризма: это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом.

Между тем российское законодательство в сфере противодействия терроризму оперирует и другими понятиями, такими как террористическая деятельность и преступления террористической направленности. Диссертант полагает, что понятие «терроризм» является родовым, исходным понятием, сущность которого конкретизируется в понятии террористической деятельности.

На сегодняшний день Федеральный закон РФ № 35-ФЗ «О противодействии терроризму» раскрывает понятие террористической деятельности посредством перечисления определенных действий, большая часть из которых находит свое отражение в УК РФ. Следует заметить, что законодательное определение террористической деятельности не соответствует требованиям юридической техники, поскольку не позволяет выделить сущностные признаки такой деятельности.

На основании проведенного анализа диссертантом предложено следующее общеправовое понятие террористической деятельности: это запрещенная Уголовным кодексом РФ и (или) Кодексом РФ об административных правонарушениях деятельность, выражающаяся в совершении деяний террористической направленности. Сущностными признаками такой деятельности являются деятельный характер (это всегда поведенческие акты), противоправность и выраженность в совершении преступлений или правонарушений террористической направленности.

Однако для целей правильного, недвусмысленного понимания террористической деятельности в контексте некоторых составов преступлений, предусмотренных главой 24 УК РФ, в примечании 1.2 к ст. 205¹ («содействие террористической деятельности») необходимо закрепить следующее понятие: «Под террористической деятельностью в статьях настоящего Кодекса следует понимать совершение хотя бы одного из преступлений, предусмотренных статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, 211 ч. 4, статьями 220, 221, 277, 278, 279, 360, 361, а также статьями 206, 209, 210, 220, 221, 281, 295, 317, 318 настоящего Кодекса, 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».

Поскольку террористическая деятельность может проявляться не только в совершении преступлений террористической направленности, но и некоторых правонарушений, следует закрепить понятие преступлений (правонарушений) террористической направленности, которые следует определять как общественно опасные, противоправные деяния, запрещенные Уголовным кодексом РФ и (или) Кодексом РФ об административных правонарушениях, которые оказывают или способствуют оказанию воздействия на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом.

Особую роль в раскрытии сущности изучаемых явлений занимает классификация, представляющая собой одно из средств (инструментов) развития научного знания. В результате проведенного исследования диссертантом была предложена классификация, основой которой выступают существенные признаки терроризма, а также классификация, основой которой выступают несущественные (но не менее значимые) признаки терроризма.

Информационный терроризм, являясь предметом изучения данного диссертационного исследования, занял свое «место» среди форм терроризма на основании двух критериев – пространства осуществления (иначе – среды протекания) и средств (инструментов), применяемых террористами, террористическими организациями (сообществами).

Информационный терроризм, являясь формой терроризма, известен российским исследователям с начала XXI в., однако до сих пор не существует единого подхода к определению его понятия и отличительных

признаков. Это обусловлено различным пониманием сущности, границ и признаков информационного пространства, выступающего специфичной платформой террористической деятельности.

В результате исследования пространства как правовой категории, а также международно-правовых и иных документов, регламентирующих вопросы предотвращения информационных угроз, диссертант разработал следующее понятие информационного пространства, ставшее основой для определения сущности информационного терроризма: это характеризующаяся безграничностью сфера существования общественных отношений, связанная с использованием информации, информационных технологий и (или) информационных ресурсов.

Отличительными признаками информационного терроризма являются следующие:

1) платформой информационного терроризма выступает информационное пространство, содержание которого было представлено выше;

2) воздействие как сущностный признак в том числе информационного терроризма обладает определенной спецификой: инструментами (средствами) воздействия выступают информация, информационные ресурсы и (или) информационные технологии.

Исходя из этого информационный терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах информационного пространства, связанного с использованием информации, информационных технологий и (или) информационных ресурсов.

Средствами информационного воздействия выступают информация, информационные технологии и информационные ресурсы.

В свою очередь, понятие «информация» являющееся исходным к понятию информационного терроризма, требует конкретизации. На основе проведенного исторического и правового анализа понятие информации как предмета или средства («орудия») совершения преступления следует определять как сведения, находящиеся на определенном носителе, обладающие информационной ценностью для своего потребителя или пользователя, использование которых необходимо для достижения преступных целей.

Понятие информационных технологий в Федеральном законе РФ «Об информации, информационных технологиях и защите информации» № 149-ФЗ следует определять как процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения *электронной* информации и способы осуществления таких процессов и методов. Кроме того, необходимо раскрыть примерный перечень таких процессов, методов поиска, сбора, хранения электронной информации для наиболее правильного применения норм специализированного законодательства, регламентирующего вопросы использования или воздействия на информационные технологии.

Соглашаясь с А.Н. Прокопенко, диссертант предлагает определять информационные ресурсы как организованную и структурированную документированную информацию, содержащуюся в библиотеках, архивах, фондах, банках данных, информационных системах.

Эффективное исследование проблем противодействия информационному терроризму лишь путем выделения его видов, которыми следует признать информационно-психологический и информационно-технологический терроризм.

Информационно-психологический терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах

информационного пространства путем совершения действий, связанных с использованием информации и оказанием влияния на сознательно-волевые компоненты личности (социальной группы либо представителя власти).

Информационно-технологический терроризм – это идеологически обоснованная практика воздействия, устрашающего население, на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах киберпространства, связанная с совершением противоправных действий в отношении отдельных компонентов информационной среды и (или) инфраструктуры государств либо организаций с помощью информационных технологий и (или) цифровых информационных ресурсов.

Создание комплекса мер противодействия информационному терроризму следует выстраивать также на основе деления его на виды.

Уголовно-правовые меры противодействия информационно-технологическому терроризму в первую очередь должны выражаться в следующем.

1. В соответствии с проведенным автором исследованием необходимо внести изменения в ч. 1 ст. 205 УК РФ и изложить ее следующим образом: «Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом либо физическим лицом и дестабилизации деятельности органа власти, органа местного самоуправления или международной организации, а также угроза совершения указанных действий в тех же целях, - наказываются...»

Дестабилизация деятельности органа власти, органа местного самоуправления или международной организации, как цель террористического акта, всегда объективно существует наравне с целью воздействия на принятие решения или совершения действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим лицом или физическим лицом. Воздействие в свою очередь проявляется не только в предъявлении требований, но и во взятии на себя ответственности за совершенные террористические акты, демонстрирующее влияние, силу и власть террористических групп (организаций или сообществ).

2. В целях повышения эффективности уголовно-правового противодействия информационно-технологическому терроризму следует предусмотреть в ч. 2 ст. 205 УК РФ пункт «г» следующего содержания:

«сопряженные с посягательством на автоматизированные системы критически важных объектов и потенциально опасных объектов государства, создающие опасность гибели человека, причинения значительного имущественного ущерба, аварийной ситуации, техногенной аварии, либо иных тяжких последствий, с помощью информационных технологий...».

3. Поскольку террористы (террористические организации, сообщества) все чаще прибегают к незаконному использованию информации для целей совершения террористических преступлений, необходимо внести изменения в содержание ст. 272, 273 УК РФ.

Часть 2 статьи 272 УК РФ изложить в следующей редакции:

«То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, а равно с целью скрыть другое преступление или облегчить его совершение, - наказывается ...».

Кроме того, необоснованной является повышенная общественная опасность ст. 273 УК РФ в сравнении со ст. 272 УК РФ, в связи с чем следует расположить квалифицирующие и особо квалифицирующие признаки ст. 273 УК РФ в той же последовательности, что и в ст. 272 УК РФ,

дифференцируя максимальное наказание по ч. 2 – до четырех лет лишения свободы, по ч. 3 – до пяти лет лишения свободы, по ч. 4 – до семи лет лишения свободы;

На основании вышеизложенного предлагается предусмотреть ч. 2 ст. 273 УК РФ в следующей редакции:

«Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, а равно с целью скрыть другое преступление или облегчить его совершение, - наказываются...».

Имея в виду возрастающую опасность распространения идеологии, составляющей основу терроризма, а равно в целях повышения эффективности уголовно-правового противодействия информационно-психологическому терроризму, следует:

1) изложить ч. 1 ст. 205² УК РФ в следующей редакции.

«Публичное оправдание террористической деятельности либо публичные призывы к осуществлению террористической деятельности, а равно распространение, изготовление хранение, перевозка, ввоз на территорию Российской Федерации или вывоз с территории Российской Федерации в целях распространения материалов с такими призывами либо материалов, оправдывающих осуществление террористической деятельности, - наказываются...».

2) следует признать чрезмерным использование в диспозиции ч. 2 ст. 205² УК РФ понятия электронные сети наравне с понятием информационно-телекоммуникационные сети, поскольку они соотносятся между собой как часть и целое. На основе вышеизложенного предлагаем изложить ч. 2 ст. 205² УК РФ в следующей редакции:

«Те же деяния, совершенные с использованием СМИ либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», - наказываются...».

3) В связи с внесенными изменениями в ч. 1 ст. 205² УК РФ, примечание 1 к ст. 205² УК РФ необходимо изложить в следующей редакции:

«в настоящей статье под публичным оправданием террористической деятельности понимается публичное признание террористической деятельности правильной, нуждающейся в поддержке и подражании».

Примечание 2 к ст. 205² УК РФ изложить в следующей редакции: «В настоящей статье под террористической деятельностью понимается совершение хотя бы одного из преступлений, предусмотренного статьями 205, 205¹, 205², 205³, 205⁴, 205⁵, 208, 211 ч.4, 220, 221, 277, 278, 279, 360, 361 настоящего Кодекса».

К комплексу иных мер противодействия информационному терроризму следует относить:

- разработку и совершенствование специализированного понятийного аппарата в сфере обеспечения информационной безопасности путем принятия и внесения изменений в правовые акты, регламентирующие вопросы защиты информации и правомерного использования информационных технологий;

- повышение эффективности сотрудничества органов и структур, направление деятельности которых связано с противодействием терроризму, с Управлением «К» МВД России и иными специализированными подразделениями, связанными с обеспечением безопасности информационно-телекоммуникационных сетей, а также с негосударственными учреждениями и организациями, деятельность которых связана с обеспечением внутренней информационной безопасности;

- разработку условий сотрудничества специализированных структур с негосударственными организациями саморегулирования СМИ по вопросу выявления публикаций, возбуждающих ненависть или вражду в отношении каких-либо социальных групп, а также публикаций, оказывающих поддержку или оправдывающих террористическую деятельность, и т.п.;

- развитие и совершенствование кадрового обеспечения информационной безопасности;

- совершенствование системы внутренней информационной защиты учреждений и организаций от возможных посягательств с помощью сети Интернет (иной локальной или территориальной сети), а также иных информационных технологий;

- установление и укрепление международного сотрудничества государств в сфере обеспечения информационной безопасности от возможных угроз террористического характера;

- иные меры превентивного характера, связанные с формированием у населения негативного отношения ко всем возможным проявлениям терроризма, к использованию насилия для достижения целей терроризма, ксенофобии и экстремизму.

Представляется, что выводы автора, включая предложения об изменении норм действующего законодательства, смогут способствовать более эффективному противодействию явлению информационного терроризма.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Нормативно-правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с изм. от 21.07.2014, № 11-ФКЗ). // Рос. газета. – 1993. – 25 дек.; СЗ РФ. – 2014. – № 31, ст. 4398.
2. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10 декабря 1948) // Рос. газета. – 1995. – 5 апреля.
3. Международный пакт от 16.12.1966 «О гражданских и политических правах» // Бюллетень Верховного Суда РФ. – 1994. – № 12.
4. Конвенция о защите прав человека и основных свобод: заключена в г. Риме 04.11.1950 (с изм. от 13.05.2004) // СЗ РФ. – 2001. – № 2, ст. 163.
5. Конвенция Совета Европы «О предупреждении терроризма»: заключена в г. Варшава 16.05.2005 // СЗ РФ. – 2009. – № 20, ст. 2393.
6. Конвенция о предотвращении и наказании преступлений против лиц, пользующихся международной защитой, в том числе дипломатических агентов: принята резолюцией 3166 (XXVIII) Генеральной Ассамблеи ООН от 14.12.1973 // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. – Вып. XXXIII. – М., 1979. – С. 90-94.
7. Модельный закон о критически важных объектах информационно-коммуникационной инфраструктуры: принят в г. Санкт-Петербурге 28.11.2014 Постановлением 41-14 на 41-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс» (по состоянию на 01.09.2016).
8. Правила Поведения в области обеспечения международной информационной безопасности от 14.09.2011: приняты на саммите Шанхайской организации сотрудничества в Астане [Электронный ресурс]. –

URL: <http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf> (дата обращения: 27.05.2016).

9. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (с изм. от 06.07.2016, № 375-ФЗ) // СЗ РФ. – 1996. – № 25, ст. 2954; 2016. – № 28, ст. 4559.

10. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (с изм. от 03.07.2016, № 354-ФЗ) // СЗ РФ. – 1994. – № 32, ст. 3301; 2016. – № 27 (ч. II), ст. 4287.

11. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (с изм. от 23.05.2016, № 146-ФЗ) // СЗ РФ. – 1996. – № 5, ст. 410; Рос. газета. – 2016. – 25 мая.

12. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (с изм. от 03.07.2016, № 314-ФЗ) // СЗ РФ. – 2006. – № 52 (1 ч.), ст. 5496; 2016. – № 27 (ч. II), ст. 4247.

13. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм. от 06.07.2016, № 205-ФЗ) // СЗ РФ. – 2002. – № 1 (ч. 1), ст. 1; 2016. – № 26 (ч. I), ст. 3874.

14. Федеральный закон РФ от 06.03.2006 № 35-ФЗ (с изм. от 06.07.2016, № 374-ФЗ) «О противодействии терроризму» // СЗ РФ. – 2006. – № 11, ст.1146; 2016. – № 28, ст. 4558.

15. Федеральный закон РФ от 25.07.2002 № 114-ФЗ (с изм. от 23.11.2015, № 314-ФЗ) «О противодействии экстремистской деятельности» // СЗ РФ. – 2002. – № 30, ст. 3031; 2015. – № 48 (ч. I), ст. 6680.

16. Федеральный закон РФ от 28.12.2010 № 390-ФЗ (с изм. от 05.10.2015, № 285-ФЗ) «О безопасности» // СЗ РФ. – 2011. – № 1, ст.2; 2015. – № 41 (ч. II), ст. 5639.

17. Федеральный закон РФ от 27.07.2006 № 149-ФЗ (с изм. от 06.07.2016, № 374-ФЗ) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 2006. – № 31 (1 ч.), ст. 3448; 2016. – № 28, ст. 4558.

18. Федеральный закон РФ от 27.07.2010 № 224-ФЗ (с изм. от 03.07.2016, № 292-ФЗ) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. – 2010. – № 31, ст. 4193; 2016. – № 27 (ч. I), ст. 4225.

19. Закон РФ от 21.07.1993 № 5458-1 (с изм. от 08.03.2015, № 23-ФЗ) «О государственной тайне» // СЗ РФ. – 1997. – № 41, ст. 8220-8235; 2015. – № 10, ст. 1395.

20. Федеральный закон Российской Федерации от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный Кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СЗ РФ. – 2016. – № 28, ст. 4559.

21. Федеральный закон РФ от 27.07.2006. № 153-ФЗ (с изм. от 06.07.2016, № 375-ФЗ) «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О ратификации Конвенции Совета Европы о предупреждении терроризма" и Федерального закона "О противодействии терроризму"» // СЗ РФ. – 2006. – № 31 (1 ч.), ст. 3452; 2016. – № 28, ст. 4559.

22. Федеральный закон РФ от 18.12.2006 № 231-ФЗ (с изм. от 29.06.2015, № 476-ФЗ) «О введении в действие части четвертой Гражданского кодекса Российской Федерации» // СЗ РФ. – 2006. – № 52 (1 ч.), ст. 5497; 2015. – № 1 (ч. I), ст. 29.

23. Федеральный закон РФ от 05.05.2014 № 130-ФЗ (с изм. от 03.07.2016, № 305-ФЗ) «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. – 2014. – №19, ст. 2335; 2016. – № 27 (ч. II), ст. 4238.

24. Федеральный закон РФ от 02.05.2015 № 116-ФЗ «О внесении изменений в статьи 13.15 и 20.29 Кодекса Российской Федерации об административных правонарушениях» // СЗ РФ. – 2015. – № 18, ст. 2619.

25. Федеральный закон РФ от 28.06.2014 № 179-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. – 2014. – №26 (ч. I), ст. 3385.

26. Федеральный закон РФ от 21.12.1994 № 68-ФЗ (с изм. от 23.06.2016, № 218-ФЗ) «О защите населения и территории от чрезвычайных ситуаций природного и техногенного характера» // СЗ РФ. – 1994. – № 35, ст. 3648; 2016. – № 26 (ч. I), ст. 3887.

27. Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 17.06.2015, № 602) «Об утверждении государственной программы Российской Федерации "Информационное общество" (2011-2020 годы)» // СЗ РФ. – 2014. – № 18 (ч. II), ст. 2159; 2015. – № 26, ст. 3896.

28. Указание Генпрокуратуры России № 65/11, МВД России № 1 от 01.02.2016 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс» (по состоянию на 01.09.2016).

29. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (зарег. в Минюсте России 30.06.2014 № 32919) // Рос. газета. – 2014. – 6 авг.

30. Концепция противодействия терроризму в Российской Федерации (утв. Указом Президента РФ 05.10.2009) // Рос. газета. – 2009. – 20 окт.

31. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Указом Президента

РФ 12.12.2014 № К 1274) [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс» (по состоянию на 01.09.2016).

32. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012 № 803) [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс» (по состоянию на 01.09.2016).

33. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 № Пр-1753) [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс» (по состоянию на 01.09.2016).

34. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Рос. газета. – 2000. – 28 сент.

35. Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (одобр. решением Президента РФ от 23.11.1995 № Пр-1694) // М.: НТЦ «Информрегистр», 1996.

36. Поручение Президента Российской Федерации от 15.11.2011 № Пр-3400 «Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года» [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс» (по состоянию на 01.09.2016).

37. Организация медико-санитарного обеспечения при террористических актах с использованием опасных химических и отравляющих веществ. Методические рекомендации (утв. Минздравом РФ 28.12.2001 № 2510/13132-01-34) // М.: ВЦМК «Защита», 2001.

38. ГОСТ 34.003-90. Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения (утв. Постановлением Госстандарта СССР от 27.12.1990 № 3399) // М.: Стандартиформ, 2009.

39. ГОСТ Р 22.0.02-94. Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий (принят Постановлением Госстандарта РФ от 22.12.1994 № 327) (с изм. от 31.05.2000, № 148-ст) // М.: Изд-во стандартов. – 1995; 2000. – ИУС «Национальные стандарты». – № 8.

40. ГОСТ 24.701-86. Государственный стандарт Союза ССР. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения (утв. Постановлением Госстандарта СССР от 31.03.1986 № 850) // М.: Изд-во стандартов. – 1986.

41. Проект Федерального закона № 1039101-6 «О внесении изменений в УК РФ и УПК РФ в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс» (по состоянию на 07.04.2016).

42. Пояснительная записка «К проекту Федерального закона "О внесении изменений в отдельные законодательные акты РФ в целях установления ответственности за публичные призывы к действиям, направленным на нарушение территориальной целостности РФ"» [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс» (по состоянию на 01.09.2016).

43. Пояснительная записка «К проекту Федерального закона "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и

обеспечению общественной безопасности"» [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс» (по состоянию на 01.09.2016).

44. Проект Конвенции об обеспечении международной информационной безопасности (концепция) [Электронный ресурс]. – URL: <http://www.scrf.gov.ru/documents/6/112.html> (дата обращения: 27.05.2016).

45. Американская конвенция о правах человека от 22 ноября 1969. [Электронный ресурс]. – URL: <http://hrlibrary.umn.edu/russian/instree/Rzoas3con.html> (дата обращения 03.08.2014).

46. Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве). Будапешт, 23.11.2001 [Электронный ресурс]. – URL: <http://mvd.gov.by/main.aspx?guid=4603> (дата обращения: 17.10.2015).

47. Федеральный закон РФ от 25.07.1998 № 130-ФЗ (с изм. от 06.03.2005) «О борьбе с терроризмом» // СЗ РФ. – 1998. – № 31, ст. 3808; утрат. силу в связи с принятием Федерального Закона от 06.03.2006 № 35-ФЗ.

48. Федеральный закон РФ от 20.02.1995 № 24-ФЗ (с изм. от 10.01.2003) «Об информации, информатизации и защите информации» // СЗ РФ. – 1995. – № 8, ст. 609; утрат. силу в связи с принятием Федерального Закона от 27.07.2006 № 149-ФЗ.

49. Computer Misuse Act 1990 [Электронный ресурс]. – URL: <http://www.legislation.gov.uk/ukpga/1990/18/section/2> (дата обращения: 27.11.2013).

50. Закон Республики Казахстан «О борьбе с терроризмом» от 13.07.1999 года № 416-1 [Электронный ресурс]. – URL: <http://mod.gov.kz> (дата обращения 27.11.2013)

51. Уголовный Кодекс Республики Узбекистан [Электронный ресурс]. – URL: http://lex.uz/pages/getact.aspx?lact_id=111457 (дата обращения 27.05.2016).

52. Закон Украины «О борьбе с терроризмом» [Электронный ресурс]. – URL: <http://www.sbu.gov.ua> (дата обращения: 27.05.2016).

53. Введение Закона о терроризм 2006 (TheterrorismAct 2006) [Электронный ресурс]. – URL: <https://www.gov.uk/government/publications/the-terrorism-act-2006> (дата обращения: 27.05.2016).

53 Уголовный кодекс Республики Казахстан (с изм. от 09.04.2016) [Электронный ресурс]. – URL: http://online.zakon.kz/Document/?doc_id=31575252 (дата обращения: 27.05.2016);

54. Уголовный кодекс Украины (с изм. от 15.03.2016) [Электронный ресурс]. – URL: <http://meget.kiev.ua/kodeks/ugolovniy-kodeks/> (дата обращения: 27.05.2016).

2. Монографии, учебная и справочная литература

55. Агапов, П.В. Уголовная ответственность за содействие террористической деятельности: тенденции современной уголовной политики [Электронный ресурс] / П.В. Агапов, К.В. Михайлов. – Саратов: Саратовский юридический институт МВД России, 2007. – 144 с. – Доступ из СПС «КонсультантПлюс».

56. Антонян, Ю.М. Криминология. Избранные лекции [Текст] / Ю.М. Антонян. – М.: «Логос», 2004. – 448 с.

57. Антонян, Ю.М. Терроризм сегодня [Текст] / Ю.М. Антонян, В.В. Смирнов. – М.: ВНИИ МВД России, 2000. – 56 с.

58. Байрамкулов, А.М. Уголовная ответственность сотрудников органов внутренних дел за преступления, совершаемые при исполнении служебных обязанностей [Текст] / А.М. Байрамкулов; под ред. Н.А. Лопашенко. – М.: Юрлитинформ, 2015. – 232 с.

59. Бачило И.Л. Информационное право: учебник [Текст] / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. – СПб.: Юридический центр Пресс, 2001. – 789 с.

- 60.** Белоножкин, В.И. Информационные аспекты противодействия терроризму [Текст] / В.И. Белоножкин, Г.А. Остапенко. – М.: Горячая линия - Телеком, 2015. – 112 с.
- 61.** Борзенков, Г.Н. Курс уголовного права. Т. 4: особенная часть [Текст] / Г.Н. Борзенков, В.С. Комиссаров. – М.: Зерцало, 2002. – 662 с.
- 62.** Борзенков, Г.Н. Курс уголовного права. Т. 5: особенная часть [Текст] / Г.Н. Борзенков, В.С. Комиссаров. – М.: Зерцало, 2002. – 502 с.
- 63.** Борьба с криминальными рынками в России [Текст] / П.В. Агапов, Л.И. Александрова, К.И. Амирбеков и др.; под общ. ред. В.В. Меркурьева. – М.: Проспект, 2015. – 312 с.
- 64.** Бояр-Созонович, Т.С. Международный терроризм: политико-правовые аспекты [Текст] / Т.С. Бояр-Созонович. – Киев-Одесса: «Лыбидь», 1991. – 163 с.
- 65.** Бояр-Созонович, Т.С. Проблема классификации современного терроризма [Текст] / Т.С. Бояр-Созонович. – М.: Университет дружбы народов им. Патриса Лумумбы, 1989. – 114 с.
- 66.** Бриллиантов, А.В. Уголовная ответственность за терроризм и захват заложников: лекция [Текст] / А.В. Бриллиантов. – М.: ИПК РК Ген. прокуратуры РФ, 2004. – 44 с.
- 67.** Будницкий, О.В. История терроризма в России в документах, библиографиях, исследованиях: учебное пособие [Текст] / О.В. Будницкий. – Ростов-на-Дону: Феникс, 1996. – 576 с.
- 68.** Бытко, Ю.И. Преступление и преступность: лекция [Текст] / Ю.И. Бытко. – Саратов, 1999. – 50 с.
- 69.** Бытко, Ю.И. Уголовное право России: части Общая и Особенная [Текст] / Ю. И. Бытко, С.Ю. Бытко; под ред. Ю.И. Бытко. – Саратов: Изд-во «Научная книга», 2011. – 314 с.
- 70.** Варыгин, А.Н. Основы криминологии и профилактики преступлений [Текст] / А.Н. Варыгин, В.Г. Громов, О.В. Шляпникова. – Саратов: изд-во Саратовского юрид. ин-та МВД России, 2000. – 128 с.

- 71.** Витюк, В.В. «Левый» терроризм на Западе: история и современность [Текст] / В.В. Витюк, С.А. Эфирова. – М.: Наука, 1987. – 320 с.
- 72.** Гаврилин, Ю.В. Современный терроризм: сущность, типология, проблемы противодействия: учебное пособие [Текст] / Ю.В. Гаврилин, Л.В. Смирнов. – М.: ЮИ МВД России, Книжный мир, 2003. – 64 с.
- 73.** Гаухман, Л.Д. Борьба с насильственными посягательствами [Текст] / Л.Д. Гаухман, В. Владимиров, Ю. Красиков. – М.: Юрид. лит., 1969. – 28 с.
- 74.** Гаухман, Л.Д. Насилие как средство совершения преступления [Текст] / Л.Д. Гаухман. – М.: Юрид. лит., 1974. – 167 с.
- 75.** Гишинский, Я.И. Криминология: теория, история, эмпирическая база, социальный контроль [Текст] / Гишинский Я.И. – СПб.: Алеф-Пресс, 2014. – 574 с.
- 76.** Грачев, С.И. Терроризм и контртеррористическая деятельность: вопросы теории: учебное пособие [Текст] / С.И. Грачев; под общ. ред. О.А. Колобова. – Нижний Новгород: ФМО/ИСИ ННГУ им. Н.И. Лобачевского, 2010. – 242 с.
- 77.** Григорьев, А.Н. Информация и информационное взаимодействие в расследовании преступлений: теоретические аспекты [Текст] / А.Н. Григорьев; ред. В.М. Мешков. – Калининград: Калининградский ЮИ МВД России, 2006. – 274 с.
- 78.** Дикаев, С.У. Террор, терроризм и преступления террористического характера (криминологическое и уголовно-правовое исследование) [Текст] / С.У. Дикаев. – СПб.: «Изд-во Юридический центр Пресс», 2006. – 486 с.
- 79.** Дуюнов, В.К. Уголовно-правовое воздействие: теория и практика [Текст] / В.К. Дуюнов. – М.: Научная книга, 2003. – 520 с.
- 80.** Емельянов, В.П. Терроризм как явление и состав преступления [Текст] / В.П. Емельянов. – Харьков: Право, 1999. – 272 с.

81. Емельянов, В.П. Терроризм и преступления с признаками терроризирования [Текст] / В.П. Емельянов. – СПб.: Изд-во Юридический центр Пресс, 2002. – 291 с.

82. Завидов, Б.Д. Ответственность за терроризм и преступления, примыкающие к нему: научно-практический и аналитический комментарий уголовного законодательства по состоянию на 12 октября 2010 года [Электронный ресурс] / Б.Д. Завидов. – Доступ из СПС «КонсультантПлюс».

83. Зеркалов, Д.В. Общественная безопасность [Электронный ресурс] / Д.В. Зеркалов. – Киев: «Основа», 2012. – URL: <http://zerkalov.kiev.ua/sites/default/files/ob-m.pdf> (дата обращения: 28.05.2016).

84. Замковой, В.И. Терроризм - глобальная проблема современности [Текст] / В.И. Замковой, М.З. Ильчиков. – М.: Фирма «Гардарика», 1996. – 75 с.

85. Информационные ресурсы развития Российской Федерации [Текст] / А.А. Антопольский, И.Л. Бачило, Г.В. Белов [и др.]; отв. ред. И.Л. Бачило – М.: Наука, 2003. – 402 с.

86. Информационные вызовы национальной и международной безопасности [Текст] / И.Ю. Алексеев, А.В. Федоров, В.Н. Цыгичко. – М.: ПИР-Центр, 2001. – 328 с.

87. Карпушин, М.П. Уголовная ответственность и состав преступления [Текст] / М.П. Карпушин, В.И. Курляндский. – М.: «Юридическая литература», 1974. – 232 с.

88. Карпец, И.И. Международная преступность [Текст] / И.И. Карпец, В.Н. Кудрявцев. – М.: Наука, 1988. – 112 с.

89. Ковалевский, В.П. Аккумуляция знаний в информационном пространстве предприятий региона [Текст] / В.П. Ковалевский, О.В. Буреш, М.А. Жук, О.М. Калиева. – М.: Финансы и статистика, 2011. – 352 с.

90. Колобов, О.А. Информационный терроризм в современном российском обществе [Текст] / О.А. Колобов, Д.В. Сочнев, М.И. Шамов. – Н. Новгород: Изд-во Нижегород. госуниверситета, 2007. – 135 с.

91. Комиссаров, В.С. Терроризм, бандитизм, захват заложника и другие тяжкие преступления против безопасности общества по новому УК РФ [Текст] / В.С. Комиссаров. – М.: Кромна-Лекс, 1997. – 159 с.

92. Кондрашов, Б.П. Общественная безопасность и административно-правовые средства ее обеспечения [Текст] / Б.П. Кондрашов. – М.: Щит-М, 1998. – 296 с.

93. Криминология: учебник для вузов [Текст] / С.В. Ванюшкин, А.Я. Гришко, Ю.Н. Демидов [и др.]; под общ. ред. А.И. Долговой. – М.: Норма, 2005. – 912 с.

94. Кроз, М.В. Криминальное психологическое воздействие [Текст] / М.В. Кроз, Н.А. Ратинова, О.Р. Онищенко. – М.: Юрлитинформ, 2008. – 200 с.

95. Кругликов, Л.Л. Преступления против личности: лекции [Текст] / Л.Л. Кругликов. – Ярославль: ЯрГУ, 1998. – 76 с.

96. Кузнецов, А.П. Преступления против основ конституционного строя и безопасности государства: учебное пособие [Текст] / А.П. Кузнецов, В.И. Булавин, С.М. Паршин. – Н. Новгород: Нижегородская правовая академия, 2006. – 80 с.

97. Кудрявцев, В.Н. Объективная сторона преступления [Текст] / В.Н. Кудрявцев. – М.: Госюриздат, 1960. – 244 с.

98. Кулапов, В.Л. Теория государства и права: учебник [Электронный ресурс] / В.Л. Кулапов. – Саратов, 2011. – URL: <http://smolsgua.ru/wp-content/uploads/2014/02/Теория-государства-и-права.pdf> (дата обращения: 28.05.2016).

99. Курс советского уголовного права: особенная часть. Т. 1 [Текст] / А.А. Пионтковский, В.Д. Меньшагин. – М.: Госюриздат, 1955. – 800 с.

100. Леонтьев, А.Н. Деятельность. Сознание. Личность. [Текст] / А.Н. Леонтьев. – М.: Политиздат, 1975. – 304 с.

101. Лопашенко, Н.А. Основы уголовно-правового воздействия: уголовное право, уголовный закон, уголовно-правовая политика [Текст] /

Н.А. Лопашенко. – СПб.: Изд-во Р. Асланова «Юридический центр Пресс», 2004. – 339 с.

102. Лопашенко, Н.А. Уголовная политика [Текст] / Н.А. Лопашенко. – М.: Волтерс Клувер, 2009. – 608 с.

103. Лунеев, В.В. Преступность XX века: мировые, региональные и российские тенденции [Текст] / В.В. Лунеев. – М.: Волтерс Клувер, 2005. – 912 с.

104. Маркс, К. Капитал: критика политической экономии: процесс капиталистического производства, взятый в целом [Электронный ресурс] / К. Маркс; под ред. Ф. Энгельс. Т. 3. Книга III. – URL: <http://www.esperanto.mv.ru/Marksismo/Kapital3/kapital3-00.html> (дата обращения: 10.05.2016).

105. Международный терроризм: борьба за геополитическое господство [Текст] / М.А. Выборнов, А.Ю. Гончаров, К.И. Поляков [и др.]; под ред. А.В. Возжеников. – М.: РАГС, 2005. – 528 с.

106. Моджорян, Л.А. Терроризм: правда и вымысел [Текст] / Л.А. Моджорян. – М.: Юрид. лит., 1983. – 208 с.

107. Назаров, М.М. Массовая коммуникация в современном мире: методика анализа и практика исследований [Текст] / М.М. Назаров. – М.: УРСС, 2000. – 239 с.

108. Нардина, О.В. Формирование общегосударственной антитеррористической системы [Текст] / О.В. Нардина. – СПб.: изд-во «Юридический центр Пресс», 2011. – 277 с.

109. Нуждин, Л.Г. Информационный терроризм [Текст] / Л.Г. Нуждин. – М.: Издательство ИКАР, 2014. – 274 с.

110. Общая теория национальной безопасности: учебник [Текст] / А.В. Важеников, И.К. Макаренко, С.А. Проскурин [и др.]; под общ. ред. А.А. Прохожева. – М.: Изд-во РАГС, 2005. – 344 с.

111. Общая теория права и государства: учебник [Текст] / М.А. Выборнов, А.Ю. Гончаров, К.И. Поляков [и др.]; под ред. В.В. Лазарева. – 3-е изд., перераб. и доп. – М.: Юристъ, 2001. – 520 с.

112. Овчинникова, Г.В. Терроризм: серия «Современные стандарты в уголовном праве и уголовном процессе» [Текст] / Г.В. Овчинников; науч. ред. Б.В. Волженкин. – СПб., 1998. – 36 с.

113. Ожегов, С.И. Словарь русского языка: около 57000 слов [Текст] / С.И. Ожегов, Н.Ю. Шведова. – 17-е изд., стереотип. – М.: Русский язык, 1985. – 797 с.

114. Ожегов, С.И. Толковый словарь русского языка [Текст] / С.И. Ожегов, Н.Ю. Шведова. – 4-е изд., дополн. – М.: Азбуковник, 1999. – 944 с.

115. Ольшанский, Д.В. Психология терроризма [Электронный ресурс] / Д.В. Ольшанский. – СПб.: Питер, 2002. – 288 с. – URL: http://scienceport.ru/files/psi_terror.pdf.

116. Панарин, И.Н. СМИ, пропаганда и информационные войны [Электронный ресурс] / И.Н. Панарин. – М., 2012. – 260 с. – URL: http://propagandahistory.ru/books/Igor-Panarin_SMI--propaganda-i-informatsionnye-voyny/ (дата обращения: 24.04.2016).

117. Петрищев, В.Е. Заметки о терроризме [Текст] / В.Е. Петрищев. – М.: Эдиториал УРСС, 2001. – 288 с.

118. Поздняков, В.А. Философия культуры [Текст] / В.А. Поздняков. – М.: Интурреклама, 1999. – 608 с.

119. Полонников, Р.И. Феномен информации и информационного взаимодействия (введение в семантическую теорию информации) [Текст] / Р.И. Полонников. – СПб.: Анатолия, 2001. – 190 с.

120. Почепцов, Г.Г. Информационные войны [Текст] / Г.Г. Почепцов. – М.: Рефл-бук; К.: Ваклер, 2000. – 280 с.

121. Пресман, А.С. Организация биосферы и ее космические связи [Текст] / А.С. Пресман. – М.: «Гео-Синтег», 1997. – 240 с.

122. Преступления против основ конституционного строя и безопасности государства: учебное пособие [Текст] / А.П. Кузнецов, В.И. Булавин, С.М. Паршин; под ред. д.ю.н., проф. А.П. Кузнецова. – Н. Новгород, 2006. – С. 80.

123. Рассолов, И.М. Право и интернет: теоретические проблемы [Электронный ресурс] / И.М. Рассолов. – М.: Норма, 2009. – 383 с. – Доступ из СПС «КонсультантПлюс».

124. Российское уголовное право [Текст] / А.В. Наумов. – 4-е изд., перераб. и доп. – Том 3. – М.: Волтерс Клувер, 2008. – 656 с.

125. Семёнова, А.В. Контент-анализ СМИ: проблемы и опыт применения [Текст] / А.В. Семёнова, М.В. Корсунская; под ред. В.А. Мансурова. – М.: Институт социологии РАН, 2010. – 324 с.

126. Сердюк, Л.В. Насилие: криминологическое и уголовно-правовое исследование [Текст] / Л.В. Сердюк; под ред. С.П. Щерба – М.: Юрлитинформ, 2002. – 384 с.

127. Словарь Ожегова: толковый словарь русского языка [Электронный ресурс]. – URL: <http://www.ozhegov.com/> (дата обращения: 14.01.2015).

128. Современный терроризм: состояние и перспективы [Текст] / В.Е. Петрищев, Ю.И. Авдеев, О.М. Хлобустов [и др.]; под ред. Е.И. Степанова. – М.: Эдиториал УРСС, 2000. – 240 с.

129. Терроризм. Правовые аспекты противодействия: нормативные и международные правовые акты с комментариями, научные статьи [Текст] / Л.К. Айвар, Ю.А. Агешин, А.В. Бриллиантов [и др.]; под ред. И.Л. Трунова, Ю.С. Горбунова. – изд. 2-е, перераб. и доп. – М.: Эксмо, 2007. – 768 с.

130. Теория государства и права: курс лекций [Текст] / М.И. Байтин, В.В. Борисов, Ф.А. Григорьев [и др.]; под ред. Н.И. Матузова, А.В. Малько. – 2-е изд., перераб. и доп. – М.: Юристъ, 2001. – 776 с.

131. Тихий, В.П. Уголовная ответственность за нарушение правил безопасности обращения с общепасными предметами [Текст] / В.П. Тихий. – Киев: Изд-во УМК ВО при Минвузе УССР, 1989. – 79 с.

132. Трайнин, А.Н. Избранные произведения. Защита мира и уголовный закон [Текст] / А.Н. Трайнин; под ред. Р.А. Руденко. – М.: Наука, 1969. – 454 с.

133. Требин, М.П. Терроризм в XXI веке [Текст] / М.П. Требин; под общ. ред. А.Е. Тараса. – Минск: Харвест, 2003. – 811 с.

134. Толковый словарь русского языка [Электронный ресурс]. – URL: <http://www.vedu.ru/expdic/33470/>

135. Толковый словарь терминов понятийного аппарата информатизации образования [Текст] / сост. И.В. Роберт, Т.А. Лавина. – М.: ИИО РАО, 2009. – 96 с.

136. Уголовное право зарубежных стран. Общая и Особенная части: учебник для магистров [Текст] / Н.А. Голованова, В.Н. Еремин, М.А. Игнатова [и др.]; под общ. ред. Н.Е. Крыловой. – 4-е изд., перераб. и доп. – М., 2013. – 1054 с.

137. Уголовное право Особенная часть: учебник для бакалавров [Электронный ресурс] / Ю.В. Грачева, А.И. Рарог, В.В. Палий [и др.]; под ред. А.И. Чучаева. М.: Проспект. – 2013. – URL: https://books.google.ru/books?id=FSw_Zrz-k7UC&printsec=frontcover&hl=ru#v=onepage&q&f=false (дата обращения: 25.05.2016).

138. Уголовное право. Общая и Особенная части: учебник для вузов [Текст] / К.Л. Акоев, С.И. Никулин, А.Е. Беяева [и др.]; под общ ред. М.П. Журавлева, С.И. Никулина. – М.: Норма, 2007. – 801 с.

139. Устинов, В.В. Международный опыт борьбы с терроризмом: стандарты и практика [Текст] / В.В. Устинов. – М.: Юрлитинформ, 2002. – 560 с.

140. Урсул, А.Д. Природа информации: философский очерк [Электронный ресурс] / А.Д. Урсул. 2-е изд. – Челябинск, 2010. – URL: http://www.inion.ru/files/File/Ursul_A_D_Priroda_informacii.pdf (дата обращения: 28.05.2016).

141. Урсул, А.Д. Природа информации. Философский очерк [Текст] / А.Д. Урсул. – М.: Политиздат, 1968. – 288 с.

142. Философия: учебник для вузов [Текст] / В.В. Васильев, П.П. Гайденко, А.Ф. Зотов [и др.]; под общ. ред. В.В. Миронова. – М.: Норма, 2005. – 928 с.

143. Федоров, В.А. Супертерроризм: новый вызов нового века [Текст] / А.В. Федоров. – М.: Права человека, 2002. – 198 с.

144. Фромм, Э. Душа человека [Текст] / Э. Фромм. – М.: ООО «Издательство АСТ»: ООО «Транзиткнига», 2004. – 572 с.

145. Хлебушкин, А.Г. Преступления экстремистской направленности в системе посягательств на основы конституционного строя Российской Федерации [Текст] / А.Г. Хлебушкин; под науч. ред. Н.А. Лопашенко. – М.: Проспект, 2015. – 192 с.

146. Черданцев, А.Ф. Теория государства и права: учебник для вузов [Текст] / А.Ф. Черданцев. – М.: Юрайт, 2002. – 432 с.

147. Шевченко, И.В. Уголовная ответственность за террористическую деятельность [Текст] / И.В. Шевченко. – М.: Юрлитинформ, 2011. – 176 с.

3. Научные статьи и другие публикации

148. Аккаева, Х.А. Характеристика терроризма в современной России и основные направления деятельности органов внутренних дел по борьбе с данным социально опасным явлением [Текст] / Х.А. Аккаева // Теория и практика общественного развития. – 2014. – № 2. – С. 419-421.

149. Алехнович, С.О. Терроризм и антитерроризм: актуальный ракурс [Текст] / С.О. Алехнович // Российский следователь. – 2007. – № 3. – С. 26-28.

150. Алиева, М.Ф. Информационная безопасность как элемент информационной культуры [Текст] / М.Ф. Алиева // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. – 2012. – № 4. – С. 96-101.

151. Амиров, В.М. Новые тенденции в освещении актов терроризма в российских печатных СМИ [Текст] / В.М. Амиров // Политическая лингвистика. – 2014. – №1. – С. 128-130.

152. Антюхов, В.И. Информационный терроризма: прошлое, настоящее, будущее [Текст] / В.И. Антюхов, А.И. Примакин, В.Е. Кадулин, Ю.И. Жуков // Вестник Санкт-Петербургского университета МВД России. – 2000. – № 1. – С. 57-64.

153. Ахиезер, А.С. Дезорганизация как категория общественной науки [Электронный ресурс] / А.С. Ахиезер // Общественные науки и современность. – 1995. – № 5. – URL: http://ecsocman.hse.ru/data/707/717/1231/004Aleksandr_AHIEZER.pdf (дата обращения: 12.05.2016).

154. Бавсун, М.Б. Понятие и содержание уголовно-правового воздействия на преступность [Текст] / М.Б. Бавсун // Вестник Томского государственного университета. – 2010. – № 336. – С. 99-102.

155. Бедрицкий, А.В. Международные договоренности по киберпространству: возможен ли консенсус? [Текст] / А.В. Бедрицкий // Проблемы национальной стратегии. – 2012. – № 4. – С. 119-136.

156. Бережан, С.Г. К семасиологической интерпретации явления синонимии [Текст] / С.Г. Бережан // Лексическая синонимия (сборник статей). – М, 1967. – С. 43-56.

157. Бойцов, А.И. Понятие насильственного преступления [Текст] / А.И. Бойцов // Криминологические и уголовно-правовые проблемы борьбы с насильственной преступностью. – Л., 1988. – № 1 (12). – С. 134-150.

158. Бугера, Н.Н. Соотношение понятий «вовлечение» и «склонение» в уголовном праве России [Текст] / Н.Н. Бугера // Юридическая наука и правоохранительная практика. – 2014. – № 3 (29). – С. 35-40.

159. Букалерева, Л.А. Уголовно-правовая охрана человека как носителя информации [Текст] / Л.А. Букалерева // Уголовное право: стратегия развития в XXI веке: сб. материалов III Международной научно-практической конференции. – М., 2006. – С. 151-154.

160. Букалерева, Л.А. Уголовная ответственность за терроризм в Индонезии [Текст] / Л.А. Букалерева, А.П. Рио // Ученые труды Российской академии адвокатуры и нотариата. – 2016. – № 2 (41). – С. 117-120.

161. Бурькова, Е.В. Профессиональная подготовка специалистов в области информационной безопасности [Текст] / Е.В. Бурькова // Вестник Оренбургского государственного университета. – 2016. – № 2(190). – С. 3-9.

162. Векленко, С.В. О повышении эффективности уголовно-правового воздействия [Текст] / С.В. Векленко // Противодействие преступности: уголовно-правовые, криминологические и уголовно-исполнительные аспекты: Материалы III Рос. конгр. уголовного права. – М., 2008. – С. 234-236.

163. Верина, Г.В. Заведомо ложное сообщение об акте терроризма в редакции майского Федерального закона 2014 года [Текст] / Г.В. Верина // Библиотека криминалиста. Научный журнал. – 2014. – № 6 (17). – С. 15-21.

164. Вершинин, М. Психологические особенности членов деструктивных и террористических (радикальных) групп [Электронный ресурс] / М. Вершинин. – URL: <http://www.follow.ru/article/339> (дата обращения: 16.04.2016).

165. Винецкий, В.Н. Криминологические аспекты изучения современных средств массовой информации и их влияния на преступность [Текст] / В.Н. Винецкий // Вестник Воронежского института МВД России. – 2011. – № 4. – С. 101-105.

166. Воронина, Т.П. Современный терроризм как феномен информационного общества [Текст] / Т.П. Воронина // Материалы II Всероссийской научно-практической Конференции. М.: Университетская книга, 2010. – Том I. – С. 446-460.

167. Галкин, А.Б. Субъективные признаки состава террористического акта [Электронный ресурс] / А.Б. Галкин // Молодой ученый. – 2014. – № 12. – С. 207-209. – URL: <http://www.moluch.ru/archive/71/12264/> (дата обращения: 20.05.2016).

168. Гарри, А. Что такое информация [Текст] / А. Гарри // Журналист. – 1928. – № 1. – С. 38-43.

169. Глотина, И.М. Информационный терроризм и его влияние на экономику [Текст] / И.М. Глотина // Проблемы современной экономики. – 2014. – № 3 (51). – С. 132-134.

170. Голубев, В.А. Проблемы борьбы с кибертерроризмом в современных условиях [Электронный ресурс] / В.А. Голубев. – URL: <http://www.crime-research.org/library/e-terrorism.htm> (дата обращения: 15.05.2016).

171. Голубев, В.А. Кибертерроризм – миф или реальность [Электронный ресурс] / В.А. Голубев. – URL: <http://www.crime-research.org/library/terror3.htm> (дата обращения: 14.05.2016).

172. Голубев, В.А. Кибертерроризм – понятие, терминология, противодействие [Электронный ресурс] / В.А. Голубев. – URL: [http://sartracc.ru/i.php?oper=read_file&filename=Pub/golubev\(17-03-05\).htm](http://sartracc.ru/i.php?oper=read_file&filename=Pub/golubev(17-03-05).htm) (дата обращения: 06.05.2016).

173. Голубин, Р.В. Место средств массовой коммуникации в борьбе с терроризмом [Текст] / Р.В. Голубин, С.И. Грачев // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2007. – №. 3. – С. 218-224.

174. Голубев, В.А. Проблемы борьбы с кибертерроризмом в современных условиях [Электронный ресурс] / В.А. Голубев, Т.А. Сайтарлы.

– URL: <http://www.crime-research.org/library/e-terrorism.htm> (дата обращения: 18.05.2016).

175. Гордеев, Н.С. Реализация принципа законности при противодействии экстремизму: теоретические и практические проблемы [Текст] / Н.С. Гордеев // Ученые записки Тамбовского отделения Рос МУ. – 2016. – № 5. – С. 73-77.

176. Гурбанов, А.Г. Общественная безопасность как объект уголовно-правовой охраны [Текст] / А.Г. Гурбанов, М.Ю. Павлик, Н.Н. Михайлов // Вестник Санкт-Петербургского университета МВД России. – 2006. – № 1. – С. 169-174.

177. Дементьева, К.В. Информационная война [Текст] / К.В. Дементьева // Журналистский ежегодник. – № 3. – 2014. – С. 14-16.

178. Дорожкин, Ю.Н. Современный терроризм: природа, особенности и средства противодействия [Текст] / Ю.Н. Дорожкин, Л.О. Изилева // Экономика и управление. – 2005. – № 1. – С. 20-27.

179. Евдокимов, К.Н. Проблема уголовно-правовой квалификации преступлений в сфере компьютерной информации [Текст] / К.Н. Евдокимов // Российский следователь. – 2012. – № 6. – С. 33-36.

180. Егорова, Н.А. Противодействие терроризму: новеллы уголовного законодательства [Текст] / Н.Е. Егорова // Криминологический журнал Байкальского государственного университета экономики и права. – 2014. – № 3. – С. 127-134.

181. Ежевская, Т.И. Психологическое воздействие информационной среды на современного человека [Текст] / Т.И. Ежевская // Психопедагогика в правоохранительных органах. – 2009. – № 2. – С. 38-41.

182. Емельянов, В.П. Понятие терроризма в уголовном законодательстве России и Украины. Сравнительный анализ [Текст] / В.П. Емельянов // Российская юстиция. – 1999. – № 11. – С. 42-43.

183. Жаглин, А.В. Общественная безопасность как социальное явление и элемент системы национальной безопасности [Текст] / А.В.

Жаглин // Вестник Воронежского института МВД России. – 2007. – № 1. – С. 31-34.

184. Жалинский, А.Э. Насильственная преступность и уголовная политика [Текст] / А.Э. Жалинский // Советское государство и право. – 1991. – № 3. – С. 101-113.

185. Закомолдин, Р.В. О тройственности понятия «общественная безопасность» в нормах действующего УК РФ [Электронный ресурс] / Р.В. Закомолдин. – URL: http://nutego.ucoz.com/index/o_trojstvennosti_ponjatija_quot_obshestvennaja_bezопасnost_quot/0-69 (дата обращения: 18.05.2016).

186. Иванов, А.К. Глобальное информационное пространство и его место в современном международном праве [Текст] / А.К. Иванов // Ползуновский вестник. – Барнаул, 2005. – № 1. – С. 219-227.

187. Ильин, Е.П. Система противодействия идеологии терроризма в Российской Федерации: становление и перспективы развития [Текст] / Е.П. Ильин // Материалы II Всероссийской научно-практической Конференции. – М.: Университетская книга, 2010. – Том I. – С. 9-21.

188. Ильин, Е.П. Доклад первого заместителя руководителя аппарата НАК [Электронный ресурс] / Е.П. Ильин // Материалы III Всероссийской научно-практической конференции «Концепция противодействия терроризму в РФ. Комплексный подход к формированию и функционированию системы противодействия распространения идеологии терроризма». – М., 2012. – URL: http://www.dagminobr.ru/storage/files/protivodeistvie%20terrorizmu/mat_vseros_konf_tom1.pdf (дата обращения: 28.05.2016).

189. Капитонова, Е.А. Особенности кибертерроризма как новой разновидности террористического акта [Текст] / Е.А. Капитонова // Известия высших учебных заведений. Поволжский регион. Общественные науки. – № 2 (34). – 2015. – С. 29-41.

190. Кардашова, И.Б. Укрепление конституционных основ общественной безопасности [Текст] / И.Б. Кардашова // Законы России: опыт, анализ, практика. – 2010. – № 4. – С. 110-114.

191. Касенова, М.Б. Трансграничное управление интернетом: основные термины и понятия [Электронный ресурс] / М.Б. Касенова // Юридический мир. – 2014. – № 2. – URL: <http://www.center-bereg.ru/h31.html> (дата обращения: 18.06.2015).

192. Каткова, М.В. Понятие «информационное пространство» в современной социальной философии [Текст] / М.В. Каткова // Известия Саратовского университета. – 2008. – № 2. – Том 8. – С. 23-26.

193. Катрич, Л.В. Проблема определения терроризма: социолингвистический анализ [Текст] / Л.В. Катрич // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2009. – № 1. – С. 18-24.

194. Кашепов, В.П. Уголовно-правовое регулирование противодействия терроризму [Текст] / В.П. Кашепов // Уголовное право. – 2006. – № 3. – С. 31-36.

195. Киреев, М.П. Исторические и современные взгляды на природу терроризма [Текст] / М.П. Киреев, С.А. Эфиоров // Уголовная политика и проблемы безопасности государства: труды академии управления МВД России. – М., 1998. – С. 42-51.

196. Колмогоров, А.Н. Три подхода к определению понятия «количество информации» [Текст] / А.Н. Колмогоров // Проблема передачи информации. – 1965. – Т. 1. – Вып. 1. – С. 3-11.

197. Комиссаров, В.С. Развитие законодательства об ответственности за терроризм в Российской Федерации [Текст] / В.С. Комиссаров; под ред. Н.А. Лопашенко // Противодействие современной преступности: оценка эффективности уголовной политики и качества уголовного закона. – Саратов: Сателлит, 2010. – С. 269-277.

198. Комиссаров, В.С. Террористический акт: уголовно-правовая характеристика основного состава [Текст] / В.С. Комиссаров // Терроризм и экстремизм в России и странах АРТ: проблемы правового регулирования и противодействия. – Владивосток: Изд-во Дальневост. федер. ун-та, 2010. – С. 7-18.

199. Корнилов, А.В. Разграничение публичных призывов к экстремистской и террористической деятельности [Текст] / А.В. Корнилов // Вестник Томского государственного университета. – 2013. – № 4(10). – С. 92-99.

200. Коробеев, А.И. Терроризм, экстремизм в современной Мексике [Текст] / А.И. Коробеев, Д.В. Лобач // Азиатско-Тихоокеанский регион: экономика, политика, право. – 2014. – № 1 (30). – С. 133-144.

201. Кочои, С.М. Общеевропейское законодательство о борьбе с терроризмом и перспективы реформирования УК РФ [Электронный ресурс] / С.М. Кочои // Lex Russica. – 2014. – №9. – С. 1061-1069. – Доступ из СПС «КонсультантПлюс».

202. Крылов, Н.Б. Государственный терроризм - угроза международной безопасности [Текст] / Н.Б. Крылов, Ю.А. Решетов // Советское государство и право. – 1987. – № 2. – С. 78-84.

203. Кудрявцев, В.Л. Склонение, вербовка или иное вовлечение лица как альтернативные действия объективной стороны содействия террористической деятельности [Текст] / В.Л. Кудрявцев // Адвокат. – 2012. – № 5. – С. 21-25.

204. Кудрявцев, В.Н. Терроризм и организованная преступность в условиях глобализации мира [Текст] / В.Н. Кудрявцев, В.В. Лунеев, В.Е. Петрищев // Борьба с терроризмом: сб. / сост. Л.В. Брятова. – М.: Наука, 2004. – С. 5-80.

205. Курс, А. Элемент интереса в информации [Текст] / А. Курс // Журналист. – 1928. – № 1. – С. 43-46.

206. Кулибаба, А.Н. Информационный терроризм [Электронный ресурс] / А.Н. Кулибаба. – URL: <http://law.edu.ru/doc/document.asp?docID=1252544> (дата обращения: 11.04.2016).

207. Кушниренко, С.П. Цифровая информация как самостоятельный объект криминалистического исследования [Электронный ресурс] / С.П. Кушниренко. – URL: <http://www.law.edu.ru/doc/document.asp?docID=1311821> (дата обращения: 12.05.2016).

208. Лабуш, Н.С. Информационная война как порождение нового времени и современных массмедиа технологий. Часть 1. Продолжение политики средствами информационного насилия [Электронный ресурс] / Н.С. Лабуш // Медиаскоп. – 2015. – № 2. – URL: <http://mediascope.ru/?q=node/1738> (дата обращения: 05.07.2016).

209. Лазарева, Н. Уголовно-правовая характеристика преступлений в области информатики и электросвязи [Текст] / Н. Лазарева // Studia Universitatis. – 2007. – С. 133-141.

210. Лапунин, М.М. Уголовная ответственность за недоносительство: история и современность [Электронный ресурс] / М.М. Лапунин // Название : сб. науч. тр. / под ред. Н.А. Лопашенко. – Саратов: Сателлит, 2006. – URL: [http://sartraccs.ru/i.php?filename=Pub/lapunin\(09-00-07\).htm&oper=read_file](http://sartraccs.ru/i.php?filename=Pub/lapunin(09-00-07).htm&oper=read_file) (дата обращения: 04.07.2016).

211. Лапунин, М.М. Противодействие терроризму в современной России: взгляд молодежи [Текст] / М.М. Лапунин // Евразийский юридический журнал. – 2009. – № 10 (17). – С. 76-84.

212. Логинов, Е.Л. Проблемы противодействия информационному терроризму [Текст] / Е.Л. Логинов // Национальные интересы: приоритеты и безопасность. – 2008. – № 4. – С. 72-76.

213. Лопаткин, Н.Ю. Организационно-правовые вопросы информационного противодействия терроризму в Российской Федерации [Текст] / Н.Ю. Лопаткин, Г.С. Чирков // Вестник РГГУ. Серия:

документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2011. – № 18 (80). – С. 271-279.

214. Лопашенко, Н.А. Разграничение лжепредпринимательства и мошенничества [Текст] / Н.А. Лопашенко // Законность. – 1997. – № 9. – С. 19-22.

215. Лунеев, В.В. Терроризм и организованная преступность: национальный и транснациональный аспекты [Текст] / В.В. Лунеев // Организованная преступность, терроризм и коррупция: криминологический ежеквартальный альманах. – 2003. – № 2. – С. 21-29.

216. Мазуров, В.А. Кибертерроризм: понятие, проблемы противодействия [Текст] / В.А. Мазуров // Доклады ТУСУРа. – 2010. – № 1. – С. 41-45.

217. Макеева, Н.В. Приоритеты уголовной политики Российской Федерации на современном этапе [Текст] / Н.В. Макеева // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2012. – № 3 (23). – С. 3-11.

218. Манойло, А.В. Информационно-психологическая война в вооруженном конфликте в Южной Осетии [Текст] / А.В. Манойло // Власть. – № 9. – 2009. – С. 81-85.

219. Методические рекомендации по совершенствованию пропагандистской работы в сфере противодействия распространению идеологии терроризма в субъектах Российской Федерации [Электронный ресурс] / под общ. ред. В.В. Попова. – М., 2013. – URL: <http://www.dgu.ru/attachments/category/60/7.pdf> (дата обращения: 26.05.2016).

220. Миньковский, Г.М. Характеристика терроризма и некоторые направления повышения эффективности борьбы с ним [Текст] / Г.М. Миньковский, В.П. Ревин // Государство и право. – 1997. – № 8. – С. 84-91.

221. Минькович, Т.В. Информационные технологии: понятийно-терминологический аспект [Текст] / Т.В. Минькович // Образовательные технологии и общество. – 2012. – № 2. – Том 15. – С. 371-389.

222. Моисеенко, А.С. О противодействии использованию сети Интернет в террористических целях [Электронный ресурс] / А.С. Моисеенко // Журнал «Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – URL: http://www.journal-nio.com/index.php?option=com_content&view=article&id=3757%3A-14&catid=114%3Amar&Itemid=157 (дата обращения: 24.05.2016).

223. Нагаева, Т.А. Применение терминов «вовлечение» и «склонение» в Российском уголовном праве [Текст] / Т.А. Нагаева // Lex Russica. – 2011. – № 3. – С. 515-539.

224. Некишев, А.В. Перспективы совершенствования модельного законодательства государств-участников СНГ в сфере противодействия технологическому терроризму [Текст] / А.В. Некишев, А.С. Клементьев // Противодействие терроризму. Проблемы XXI века - Counter-Terrorism. – 2015. – № 4. – 36-40.

225. Нестеров, С.В. Понятие общественной безопасности [Текст] / С.В. Нестеров // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2013. – № 11 (127). – С. 2-8.

226. Новикова, Е. Использование ограничения свободы в санкциях за преступления в сфере компьютерной информации [Электронный ресурс]. – URL: https://zakon.ru/blog/2012/2/26/ispolzovanie_ogranicheniya_svobody_v_sankciyax_za_prestupleniya_v_sfere_kompyuternoj_informacii (дата обращения: 23.05.2016).

227. Номоконов, В.А., Тропина, Т.Л. Киберпреступность как новая криминальная угроза [Текст] / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45-55.

228. Паненков, А.А. Борьба с финансированием террористической деятельности в России [Электронный ресурс] / А.А. Паненков // Право и безопасность. – 2009. – № 3 (32). – URL: http://dpr.ru/pravo/pravo_28_16.htm (дата обращения: 27.05.2016).

229. Пархоменко, С.В. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подход [Текст] / С.В. Пархоменко, К.Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – Т. 9. – № 2. – С. 265-276.

230. Петрищев, В.Е. Защита объектов террористических посягательств и проблемы информационного противоборства [Текст] / В.Е. Петрищев // Организованный терроризм и организованная преступность. – М.: Рос. криминолог. ассоц., 2002. – С. 33-47.

231. Петрищев, В.Е. Противодействие террористической идеологии - приоритетное направление профилактики терроризма [Электронный ресурс] / В.Е. Петрищев. // II Всероссийская научно-практическая Конференция в МГУ им. М.В. Ломоносова. – М., 2010. – URL: <http://nac.gov.ru/publikacii/stati-knigi-broshyury/petrishchev-ve-protivodeystvie.html> (дата обращения: 09.11.2015).

232. Пинкевич, Т.В. Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма: проблемы квалификации [Текст] / Т.В. Пинкевич // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2014. – № 3. – С. 141-144.

233. Побегайло, Э.Ф. Терроризм и уголовная ответственность [Текст] / Э.Ф. Побегайло // Актуальные проблемы Европы. Проблемы терроризма: Проблемно-тематический сборник. – 1997. – № 4. – С. 197-203.

234. Попов, Д.В. К вопросу о соотношении уголовно-правовых понятий: принуждение и насилие [Текст] / Д.В. Попов // Актуальные вопросы уголовного процесса современной России.–Уфа, 2003.–С. 44-51.

235. Попов, В.Г. О концепции государственного управления и регулирования противодействия терроризму [Текст] / В.Г. Попов, В.А. Коношенко, Г.И. Чиров // Борьба с терроризмом: актуальные проблемы

законодательного обеспечения: сб. науч. ст. – Ростов н/Д: РЮИ МВД России, 2003. – С. 84-89.

236. Прокопенко, А.Н. О содержании понятия информационные ресурсы в праве [Текст] / А.Н. Прокопенко // Бизнес в законе. Экономико-юридический журнал. – 2010. – № 1. – С. 157-160.

237. Путилин, Б.Г. Кризис и международный терроризм [Текст] / Б.Г. Путилин // Материалы Конференции в ИМЭМО РАН, 20-21 апреля 2009 «Глобальный кризис и проблемы обеспечения общественно-политической стабильности: опыт стран Запада и Россия» / ред. Н.В. Загладин. – М., ИМЭМО РАН, 2009. – С. 124-129.

238. Разгильдиев, Б.Т. Уголовно-правовое воздействие и его пределы [Текст] / Б.Т. Разгильдиев // Известия вузов. Правоведение. – 2011. – № 2. – С. 174-179.

239. Рассолов, И.М. Киберпреступность: понятие, основные черты, формы проявления [Электронный ресурс] / И.М. Рассолов // Юридический мир. Общероссийский научно-практический правовой журнал. – М.: Юрист. – 2008. – № 2 (134). – Доступ из СПС «КонсультантПлюс».

240. Робинов, А.А. Ограничение свободы СМИ и борьба с терроризмом [Текст] / А.А. Робинов // Журнал российского права. – 2003. – № 5. – С. 103-108.

241. Роговский, Е.А. Россия в борьбе с международным терроризмом: грани повышения позитивного образа страны [Электронный ресурс] / Е.А. Роговский // Электронный научный журнал «Россия и Америка в XXI веке». – 2007. – №3. – URL: <http://www.rusus.ru/?act=read&id=66> (дата обращения: 11.04.2016).

242. Россошанский, А.В. Риски и угрозы информационного терроризма [Текст] / А.В. Россошанский // Человек. Сообщество. Управление. – 2011. – № 3. – С. 100-108.

243. Савостицкий, Ю.А. История развития глобальных компьютерных сетей [Текст] / Ю.А. Савостицкий // Информационное общество. – 2000. – № 4. – С. 59-65.

244. Сапожонкова, А.А. Интернет как инструментальное средство терроризма [Текст] / А.А. Сапожонкова // Международный научно-исследовательский журнал. – 2014. – № 12-2 (31). – С. 61-62.

245. Семькин, Н. Создание террористических групп необходимо криминализовать в УК всех государств Содружества [Текст] / Н. Семькин // Российская юстиция. – 2003. – № 1. – С. 66.

246. Сидоров, Б.В. Терроризм и террористическая деятельность: вопросы соотношения, системный анализ и проблема совершенствования уголовно-правового и криминологического противодействия [Текст] / Б.В. Сидоров // Вестник экономики, права и социологии. – 2015. – № 4. – С. 234-243.

247. Сидоров, П.И. Психический терроризм как форма несмертоносного оружия [Текст] / П.И. Сидоров // Экология человека. – 2005. – № 7. – С. 12-17.

248. Скакунов, Э.И. Политические конфликты в современных условиях [Текст] / Э.И. Скакунов, В.Е. Насиновский // США: экономика, политика, идеология. – 1995. – № 4. – С. 3-14.

249. Соловьев, А.В. Информационная война: понятие, содержание, перспектива [Текст] / А.В. Соловьев // Пространство и время. – 2010. – № 2. – С. 75-79.

250. Солопанов, Ю.В. Об ответственности за недонесение о готовящемся или совершенном преступлении [Электронный ресурс] / Ю.В. Солопанов. – URL: <http://law.edu.ru/article/article.asp?articleID=158462> (дата обращения 04.07.2016).

251. Сочнев, Д.В. Основные виды и наиболее распространенные формы международного терроризма [Электронный ресурс] / Д.В. Сочнев,

М.М. Абасов // Полицейская и следственная деятельность. – 2013. – № 2. – URL: http://e-notabene.ru/pm/article_801.html (дата обращения 02.10.2015).

252. Старостина, Е.В. Терроризм и кибертерроризм: угроза международной безопасности [Электронный ресурс] / Е.В. Старостина. – URL: <http://www.crime-research.ru/articles/starostina/3> (дата обращения: 11.04.2016).

253. Старостина, Е.В. Проблема выработки единого понятия «кибертерроризм» и состав правонарушения в Российском законодательстве [Текст] / Е.В. Старостина // Научная сессия МИФИ. – 2006. – Том 14. – С. 111-113.

254. Степанов, О.А. Ключевые аспекты правового регулирования использования и развития информационно-электронных технологий [Текст] / О.А. Степанов // Государство и право. – 2004. – № 4. – С. 70-72.

255. Степанов-Егиянц, В.Г. Субъективная сторона компьютерных преступлений [Текст] / В.Г. Степанов-Егиянц // Бизнес в законе. Экономико-юридический журнал. – 2013. – № 2. – 72-75.

256. Сундиев, И.Ю. Новое качество террористической пропаганды: медиа империя ИГИЛ [Электронный ресурс] / И.Ю. Сундиев, А.А. Смирнов, В.Н. Костин. – URL: <http://spkurdyumov.ru/biology/novoe-kachestvo-terroristicheskoy-propagandy-mediamperiya-igil/> (дата обращения: 15.11.2015).

257. Сундиев, И.Ю. Сетевые возможности и сетевые угрозы: информационные сети в экстремистской и террористической деятельности [Текст] / И.Ю. Сундиев, А.А. Смирнов // Свободная мысль - XXI. – 2013. – № 5. – С. 191-204.

258. Тарбагаев, А.Н. Проблемы уголовно-правовой квалификации терроризма [Электронный ресурс] / А.Н. Тарбагаев // Криминологический журнал Байкальского государственного университета экономики и права. – URL: <http://cj.isea.ru/reader/article.asp?id=16519> (дата обращения: 14.03.2016).

259. Тасаков, С.В. Развратные действия в сети Интернет [Текст] / С.В. Тасаков, Р.М. Кочетов // Уголовное право. – 2014. – № 5. – С. 96-97.

260. Тимофеева, Н.Ю. К вопросу об определении терроризма в работах зарубежных правоведов [Текст] / Н.Ю. Тимофеева // Государство и право России: история и современность. – 2008. – № 3. – С. 87-92.

261. Туронок, С.Г. Информационный терроризм: выработка стратегии противодействия [Текст] / С.Г. Туронок // Общественные науки и современность. – 2011. – № 4. – С. 131-140.

262. Фарвазова, Ю.Р. Актуальные аспекты совершенствования правового регулирования незаконного использования информационного пространства в террористических целях [Текст] / Ю.Р. Фарвазова // Армия и общество. – 2013. – №5. – С. 18-23.

263. Федорова, О.Н. Роль информационно-психологической безопасности граждан в России [Текст] / О.Н. Федорова // Гуманитарные и социальные науки. – 2012. – № 2. – С. 342-355.

264. Фомина, Л.Ю. Обеспечение единства терминологии нормативных правовых актов: проблемы и перспективы [Текст] / Л.Ю. Фомина // Социально-политические науки. – 2012. – № 1. – С. 96-100.

265. Чернявский, Д.О. Публичные призывы к нарушению территориальной целостности: проблемы социально-политической обусловленности уголовно-правового запрета [Текст] / Д.О. Чернявский, Р.М. Скулаков // Юридическая наука и правоохранительная практика. – 2015. – № 1(31). – С. 73-79.

266. Чубик, А.П. Терроризм в информационном пространстве [Текст] / А.П. Чубик // Известия Томского политехнического университета. – 2013. – № 6. – Т. 323. – С. 117-120.

267. Шоткинов, С.А. СМИ и преступность: специфика взаимодействия [Текст] / С.А. Шоткинов // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2003. – № 1(6). – С. 239-250.

4. Диссертации и авторефераты диссертаций

268. Айсанов, Р.М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном законодательстве [Текст] / Р.М. Айсанов: дис. ... канд. юрид. наук. – М., 2006. – 191 с.

269. Асланян, Р.Г. Информация как предмет и средство совершения преступления в сфере экономической деятельности [Текст] / Р.Г. Асланян: дис. ... канд. юрид. наук. – Краснодар, 2016. – 176 с.

270. Алексеев, О.Н. Международный терроризм и борьба с ним крупнейших государств тихоокеанского региона [Текст] / О.Н. Алексеев: дис. ... канд. политич. наук. – Владивосток, 2013. – 206 с.

271. Арзамасцев, Н.И. Административно-правовое обеспечение органами внутренних дел общественной безопасности при чрезвычайных ситуациях техногенного характера [Текст] / Н.И. Арзамасцев: дис. ... канд. юрид. наук. – М., 2002. – 162 с.

272. Бабошин, К.И. Социально-политическая стабильность в современной России: социологический анализ [Текст] / К.И. Бабошин: дис. ... канд. философ. наук. – Саратов, 2005. – 144 с.

273. Бахтеева, А.Р. Политический терроризм как социальное явление современности [Текст] / А.Р. Бахтеева: автореф. дис. ... канд. социолог. наук. – М., 2010. – 23 с.

274. Белая, Е.В. Феномен терроризма в современном обществе [Текст] / Е.В. Белая: дис. ... канд. социол. наук. – М., 2005. – 153 с.

275. Белявский, Д.Г. Детерминанты терроризма как социально-правового явления [Текст] / Д.Г. Белявский: автореф. дис. ... канд. юрид. наук. – М., 2007. – 32 с.

276. Бобраков, И.А. Воздействие преступников на свидетелей и потерпевших и криминалистические методы его преодоления [Текст] / И.А. Бобраков: дис. ... канд. юрид. наук. – М., 1997. – 210 с.

277. Боровский, А.С. Модели, методы и алгоритмы интеллектуальной поддержки принятия решений в задачах разработки и оценки систем

физической защиты объектов информатизации [Текст] / А.С. Боровский: автореф. дис. ... д-ра технич. наук. – СПб., 2015. – 34 с.

278. Букалерева, Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы [Текст] / Л.А. Букалерева: дис. ... д-ра. юрид. наук. – М., 2007. – 574 с.

279. Бытко, С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерной информации [Текст] / С.Ю. Бытко: дис. ... канд. юрид. наук. – Саратов, 2002. – 204 с.

280. Василенко, В.В. Международный терроризм в условиях глобального развития (политический анализ) [Текст] / В.В. Василенко: дис. ... д-ра. юрид. наук. – М., 2003. – 311 с.

281. Великосельский, М.Ю. Дискурс феномена терроризма в СМИ США [Текст] / М.Ю. Великосельский: дис. ... канд. политич. наук. – СПб., 2011. – 190 с.

282. Дерюгина, Ю.Н. Терроризм: уголовно-правовой и криминологический аспекты [Текст] / Ю.Н. Дерюгина: дис. ... канд. юрид. наук. – М., 2001. – 252 с.

283. Джакупов, Ж.А. Формирование и развитие единого информационного пространства юридического сообщества Российской Федерации (на примере ассоциации юристов России) [Текст] / Ж.А. Джакупов: автореф. дис. ... канд. юрид. наук. – М., 2011. – 22 с.

284. Дремлюга, Р.И. Интернет-преступность [Текст] / Р.И. Дремлюга: дис. ... канд. юрид. наук. – Владивосток, 2007. – 248 с.

285. Евдокимов, К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации (по материалам Восточно-Сибирского региона) [Текст] / К.Н. Евдокимов: дис. ... канд. юрид. наук. – Иркутск., 2006. – 203 с.

286. Ефанова, Е.В. Терроризм как фактор политической дестабилизации современного российского общества [Текст] / Е.В. Ефанова: дис. ... канд. политич. наук. – Волгоград, 2006. – 191 с.

287. Журавлев, Д.А. Международный терроризм в информационно-коммуникативном пространстве мировой политики [Текст] / Д.А. Журавлев: дис. ... канд. политич. наук. – М., 2011. – 286 с.

288. Григорьев, А.А. Уголовно-правовая ответственность за терроризм в современном праве Российской Федерации [Текст] / А.А. Григорьев: дис. ... канд. юрид. наук. – Челябинск, 2012. – 217 с.

289. Гриб, Н.Н. Криминологические аспекты противодействия терроризму в современной России [Текст] / Н.Н. Гриб: автореф. дис. ... канд. юрид. наук. – СПб., 2005. – 20 с.

290. Грибанов, Д.В. Правовое регулирование кибернетического пространства как совокупности информационных отношений [Текст] / Д.В. Грибанов: дис. ... канд. юрид. наук. – Екатеринбург, 2003. – 227 с.

291. Кубышкин, А.В. Международно-правовые проблемы обеспечения информационной безопасности государств [Текст] / А.В. Кубышкин: дис. ... канд. юрид. наук. – М., 2002. – 193 с.

292. Коссе, В.О. Терроризм: социально-генетический и типологический анализ [Текст] / В.О. Коссе: дис. ... канд. философ. наук. – Нижний Новгород, 2004. – 149 с.

293. Кривоухов, А.А. Правовое регулирование защиты государственных информационных ресурсов [Текст] / А.А. Кривоухов: дис. ... канд. юрид. наук. – Воронеж, 2006. – 224 с.

294. Лазарев, Н.Я. Терроризм как социально-политическое явление: истоки, формы и динамика развития в современных условиях [Текст] / Н.Я. Лазарев: автореф. дис. ... канд. политич. наук. – М., 2007. – 26 с.

295. Лунёв, А.А. Терроризм как объект криминологического изучения [Текст] / А.А. Лунёв: дис. ... канд. юрид. наук. – Ростов-на-Дону, 2004. – 180 с.

296. Макиенко, А.В. Уголовно-правовые и криминологические проблемы предупреждения криминогенного информационного воздействия преступных сообществ [Текст] / А.В. Макиенко: дис. ... канд. юрид. наук. – М., 1997. – 187 с.

297. Мардоян, А.В. Терроризм как международное преступление [Текст] / А.В. Мардоян: дис. ... канд. юрид. наук. – М., 2007. – 198 с.

298. Малыковцев, М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ [Текст] / М.М. Малыковцев: дис. ... канд. юрид. наук. – М., 2007. – 186 с.

299. Маляров, А.И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации [Текст] / А.И. Маляров: автореф. дис. ... канд. юрид. наук. – Краснодар, 2008. – 26 с.

300. Матчанова, З.Ш. Факторы распространения терроризма в современной России: криминологический анализ [Текст] / З.Ш. Матчанова: дис. ... канд. юрид. наук. – СПб., 2015. – 229 с.

301. Менжега, М.М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ [Текст] / М.М. Менжега: дис. ... канд. юрид. наук. – Саратов, 2005. – 238 с.

302. Мещерякова, С.Н. Российские средства массовой информации в институционально-правовом обеспечении межнационального согласия: дис. ... канд. юрид. наук. – Ростов-на-Дону, 2005. – 145 с.

303. Моисеенко, А.И. Уголовно-правовая и криминологическая характеристика терроризма (по материалам Южного федерального округа России) [Текст] / А.И. Моисеенко: дис. ... канд. юрид. наук. – Ставрополь, 2006. – 192 с.

304. Молодчая, Е.Н. Политика противодействия кибертерроризму в современной России: политологический аспект [Текст] / Е.Н. Молодчая: дис. ... канд. политич. наук. – М., 2011. – 188 с.

305. Мусаелян, М.Ф. Террористический акт: уголовно-правовой аспект [Текст] / М.Ф. Мусаелян: дис. ... канд. юрид. наук. – М., 2007. – 226 с.

306. Назаркин, М.В. Криминологическая характеристика и предупреждение терроризма [Текст] / М.В. Назаркин: дис. ... канд. юрид. наук. – М., 1998. – 197 с.

307. Никитин, А.В. Терроризм как форма девиантного поведения (криминологический аспект) [Текст] / А.В. Никитин: автореф. дис. ... канд. юрид. наук. – СПб., 2003. – 19 с.

308. Палий, В.В. Вовлечение в совершение преступления и склонение к совершению преступлений или антиобщественных действий [Текст] / В.В. Палий: автореф. дис. ... канд. юрид. наук. – М., 2006. – 188 с.

309. Пилипенко, С.П. Институт обстоятельств, отягчающих наказание, в уголовном законодательстве (теоретико-прикладной анализ) [Текст] / С.П. Пилипенко: автореф. дис. ... канд. юрид. наук. – Нижний Новгород, 2007. – 31 с.

310. Попов, И.В. География современного терроризма в странах европейского союза [Текст] / И.В. Попов: дис. ... канд. географич. наук. – М., 2009. – 232 с.

311. Радостева, Ю.В. Уголовно-правовое понятие насилия [Текст] / Ю.В. Радостева: дис. ... канд. юрид. наук. – Екатеринбург, 2006. – 165 с.

312. Рыбалкин, Н.Н. Природа безопасности [Текст] / Н.Н. Рыбалкин: автореф. дис. ... канд. философ. наук. – М., 2003. – 44 с.

313. Резяпова, Г.Ф. Терроризм как социальное явление [Текст] / Г.Ф. Резяпова: автореф. дис. ... канд. философ. наук. – Уфа, 2005. – 19 с.

314. Салихов, И.И. Информация с ограниченным доступом как объект гражданских правоотношений [Текст] / И.И. Салихов: дис. ... канд. юрид. наук. – Казань, 2004. – 274 с.

315. Салихов, И.И. Информация с ограниченным доступом как объект гражданских правоотношений [Текст] / И.И. Салихов: автореф. дис. ... канд. юрид. наук. – Казань, 2004. – 38 с.

316. Семёнов, З.Х. Особенности освещения явления «международный терроризм» в газетной периодике России [Текст] / З.Х. Семёнов: дис. ... канд. философ. наук. – М., 2006. – 177 с.

317. Солдаткина, О.Л. Информационные ресурсы российской правовой политики: общетеоретический аспект [Текст] / О.Л. Солдаткина: дис. ... канд. юрид. наук. – Саратов, 2001. – 188 с.

318. Соломин, Д.А. Противодействие терроризму в информационной сфере [Текст] / Д.А. Соломин: дис. ... канд. политич. наук. – М., 2004. – 197 с.

319. Сопов, Д.В. Уголовная ответственность за терроризм: проблемы квалификации [Текст] / Д.В. Сопов: дис. ... канд. юрид. наук. – М., 2004. – 203 с.

320. Сорока, Е.Ю. Особенности и тенденции эволюции современного терроризма [Текст] / Е.Ю. Сорока: дис. ... канд. политич. наук. – М., 2006. – 196 с.

321. Столяров, А.В. Информационная свобода и информационное насилие [Текст] / А.В. Столяров: дис. ... канд. философ. наук. – М., 2012. – 155 с.

322. Телешина, Н.Н. Виртуальное пространство как объект контрольной деятельности государства [Текст] / Н.Н. Телешина: автореф. дис. ... канд. юрид. наук. – Муром, 2011. – 26 с.

323. Тисленко, Д.И. Экологический терроризм: уголовно-правовые и криминологические проблемы [Текст] / Д.И. Тисленко: дис. ... канд. юрид. наук. – Тамбов, 2011. – 250 с.

324. Тропина, Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы [Текст] / Т.Л. Тропина: дис. ... канд. юрид. наук. – Владивосток, 2005. – 235 с.

325. Турышев, А.А. Информация как признак преступлений в сфере экономической деятельности [Текст] / А.А. Турышев: дис. ... канд. юрид. наук. – Омск, 2006. – С. 210 с.

326. Федоров, А.Ю. Криминальное манипулирование в сфере экономической деятельности: криминологическая характеристика и предупреждение [Текст] / А.Ю. Федоров: автореф. дис. ... канд. юрид. наук. – Омск, 2006. – 25 с.

327. Федорцев, В.А. Негосударственный терроризм как форма политической борьбы: основные признаки и тенденции исторического развития [Текст] / В.А. Федорцев: дис. ... канд. политич. наук. – М., 2007. – 166 с.

328. Шамов, М.И. Государственная стратегия и политические технологии предупреждения информационного терроризма в современном российском обществе [Текст] / М.И. Шамов: автореф. дис. ... канд. политич. наук. – Нижний Новгород, 2007. – 24 с.

329. Шамов, М.И. Государственная стратегия и политические технологии предупреждения информационного терроризма в современном российском обществе [Текст] / М.И. Шамов: дис. ... канд. политич. наук. – Нижний Новгород, 2007. – 179 с.

330. Шарапов, А.К. Политический терроризм: развитие ресурсного потенциала и типология [Текст] / А.К. Шарапов: дис. ... канд. политич. наук. – Чита., 2005. – 206 с.

331. Шевченко, И.В. Уголовная ответственность за террористическую деятельность: уголовно-правовой и правоприменительный аспекты [Текст] / И.В. Шевченко: дис. ... канд. юрид. наук. – Тамбов, 2010. – 224 с.

332. Яковлева, И.А. Информация с ограниченным доступом в предпринимательской деятельности: правовой аспект [Текст] / И.А. Яковлева: автореф. дис. ... канд. юрид. наук. – М., 2014. – 24 с.

333. Ярославцева, А.О. Политическая стабильность и конфигурации политической элиты: интерпретативный потенциал и границы применимости теоретических походов [Текст] / А.О. Ярославцева: дис. ... канд. политич. наук. – М., 2012. – 169 с.

334. Яшков, С.А. Информация как предмет преступления [Текст] / С.А. Яшков: дис. ... канд. юрид. наук. – Екатеринбург, 2005. – 151 с.

5. Статистические данные

335. Краткая характеристика состояния преступности в Российской Федерации за январь - июнь 2016 года. [Электронный ресурс]. – URL: <https://мвд.рф/folder/101762/item/8127775/> (дата обращения: 26.05.2016).

336. Состояние преступности – январь - декабрь 2015 года [Электронный ресурс]. – URL: <https://мвд.ру/folder/101762/item/7087734/> (дата обращения: 18.05.2016).

337. Состояние преступности в России за январь - июнь 2016 года [Электронный ресурс]. – URL: <http://crimestat.ru/analytics> (дата обращения: 26.05.2016).

338. Состояние преступности в России за январь - декабрь 2015 года [Электронный ресурс]. – URL: <http://crimestat.ru/analytics> (дата обращения: 26.05.2016).

6. Электронные ресурсы

339. Бенитес Х., Хили Д. США. Воздушные замки кибербезопасности [Электронный ресурс]. – URL: <http://topwar.ru/18781-vozdushnye-zamki-kiberbezopasnosti.html> (дата обращения: 28.05.2016).

340. Бондарь Ю.М. Иран: январь 2012. Военно-политическая ситуация [Электронный ресурс]. – URL: <http://www.iimes.ru/rus/stat/2012/27-02-12d.htm> (дата обращения: 21.05.2016).

341. Владимир Путин обеспокоен вовлечение в ИГИЛ граждан России [Электронный ресурс]. – URL: <http://www.pravmir.ru/vladimir-putin-obespokoen-vovlecheniem-v-igil-grazhdan-rossii/> (дата обращения 06.11.2015).

342. В. Путин предупредил США, что нельзя прибегать к помощи террористов [Электронный ресурс]. – URL: <http://www.kp.ru/online/news/2040147/> (дата обращения: 24.05.2015).

343. BBC Шри-Ланки разбомбили радио «тамильских тигров» [Электронный ресурс]. – URL: <https://lenta.ru/news/2007/11/27/station/> (дата обращения: 11.05.2016).

344. В Совете Федерации обсудили проблему информационного терроризма [Электронный ресурс]. – URL: <http://scienceport.ru/anlytics/v-sovete-federatsii-obsudili-problemu-informatsionnogo-terrorizma/> (дата обращения: 12.05.2016).

345. Выступление первого заместителя руководителя аппарата НАК Е.П. Ильина на Всероссийском семинаре-совещании руководителей патриотических объединений от 27 октября 2015 [Электронный ресурс]. – URL: <http://nac.gov.ru/publikacii/vystupleniya-i-intervyu/vystuplenie-pervogo-zamestitelya.html> (дата обращения: 06.11.2015).

346. Выступление председателя национального антитеррористического комитета, директора ФСБ России А.В. Бортникова на открытии совместного заседания НАК и ФОИШ. Москва, 15.12.2015 [Электронный ресурс]. – URL: <http://nac.gov.ru/publikacii/vystupleniya-i-intervyu/vystuplenie-predsedatelya-nacionalnogo-0.html> (дата обращения: 08.07.2016).

347. Глава ФСБ: по фактам финансирования терроризма возбуждено 270 уголовных дел [Электронный ресурс]. – URL: <http://regnum.ru/news/polit/2036140.html> (дата обращения: 24.05.2016).

348. Данные клиентов «Приват-банка» выложили в Сеть [Электронный ресурс]. – URL: <https://life.ru/t/новости/135943> (дата обращения 17.05.2016).

349. Движение «Хезболлах» [Электронный ресурс]. – URL: <http://ria.ru/spravka/20130610/942487146.html> (дата обращения: 11.05.2016).

350. Деятельность ENISA за октябрь 2015 [Электронный ресурс]. – URL: <http://d-russia.ru/deyatelnost-enisa-za-oktyabr-2015-goda.html> (дата обращения: 08.07.2016).

351. Ермаков Г. Telegram содержит 30-40 каналов ИГИЛ, используемых террористами для пропаганды [Электронный ресурс]. – URL: <http://www.3dnews.ru/923839> (дата обращения: 11.05.2016).

352. Ермаков С. Ядерное оружие вытеснят информационные технологии [Электронный ресурс]. – URL: http://www.pravda.ru/news/expert/15-12-2014/1240108-Sergey_Ermakov-0/ (дата обращения: 14.04.2016).

353. Информационная безопасность критически важных объектов [Электронный ресурс]. – URL: http://www.it.ru/press_center/publications/7353/ (дата обращения: 16.11.2015).

354. Использование интернета в террористических целях // Управление Организации Объединенных Наций по наркотикам и преступности. Нью-Йорк, 2013. С. 10. [Электронный ресурс]. – URL: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf (дата обращения: 20.05.2016).

355. История появления терроризма [Электронный ресурс]. – URL: <http://www.privacyandterrorism.org/history.php> (дата обращения: 11.04.2016).

356. Как современные террористы используют Интернет. [Электронный ресурс]. – URL: <http://www.alphagroup.kz/ru/media-files/stati/39-kak-sovremennye-terroristy-ispolzujut-internet> (дата обращения: 07.05.2016).

357. Кибератака реальной войны [Электронный ресурс]. – URL: http://www.e-reading.club/chapter.php/75936/106/Kurushin_-_100_velikih_voennyh_tain.html (дата обращения: 17.05.2016).

358. Козловский В. В США обнародованы материалы, изъятые у бин Ладена [Электронный ресурс]. – URL:

http://www.bbc.com/russian/international/2015/05/150521_osama_bin_laden_library (дата обращения 15.05.2016).

359. Количество пользователей интернет России. Обновление от 09.06.2015 года [Электронный ресурс]. – URL: http://www.bizhit.ru/index/users_count/0-151 (дата обращения 12.05.2016).

360. Курс «Мировые информационные ресурсы» [Электронный ресурс]. – URL: <http://mir.it-karma.ru/teoreticeskie-osnovy-informacionnyh-resursov/lekcii/1-osnovnye-ponatia-i-susnost-informacionnyh-resursov> (дата обращения: 26.05.2016).

361. Лекция по террологии [Электронный ресурс]. – URL: <http://www.mylect.ru/polytolog/obchee/434-terrologiya.html> (дата обращения: 27.05.2016).

362. МВД Зарегистрировало около 11 000 киберпреступлений в 2014 г. [Электронный ресурс]. – URL: <http://www.vedomosti.ru/technology/articles/2015/02/06/kiberprestupniki-v-spiskah-ne-znachatsya> (дата обращения: 17.11.2015).

363. Мухачев С.В. Динамика информационных компьютерных преступлений [Электронный ресурс]. – URL: <http://www.mvd.informost.ru/2012/pdf/part1/1-27.pdf> (дата обращения: 17.11.2015).

364. Нарышкин Сергей назвал главные цели террористов. [Электронный ресурс]. – URL: <http://govoritmoskva.ru/news/59758/> (дата обращения 08.03.2016)

365. Новые риски финансирования терроризма [Электронный ресурс] // Группа разработки финансовых мер борьбы с отмыванием денег. – 2015. – С. 23. – URL: http://www.cbr.ru/today/anti_legalisation/fatf/Emerging-Terrorist-Financing-Risks_Russian.pdf (дата обращения: 17.05.2016).

366. Одна из ведущих компаний в мире по предотвращению и расследованию киберпреступлений и мошенничеств с использованием

высоких технологий [Электронный ресурс]. – URL: <http://www.group-ib.ru> (дата обращения 09.04.2013).

367. Обобщенные результаты социологического исследования по вопросам противодействия идеологии терроризма в 2012 году // Российский государственный университет нефти и газа имени И.М. Губкина. [Электронный ресурс]. – URL: <http://scienceport.ru/files/soc-isledovaniya-2012.pdf> (дата обращения: 14.06.2015).

368. Парижские террористы использовали для связи PlayStation 4 [Электронный ресурс]. – URL: <http://rsute.ru/obshestvo/51625.html> (дата обращения 17.11.2015).

369. Петров М.Н. Как уничтожить террористов. Действия штурмовых групп [Электронный ресурс]. – URL: <http://coollib.com/b/266884> (дата обращения: 11.04.2016).

370. Пользование интернетом в России: итоги 2014 года [Электронный ресурс]. – URL: https://www.gfk.com/fileadmin/user_upload/dyna_content/RU/Documents/News/2015/Internet_in_Russia_2014-final_full.pdf (дата обращения: 16.11.2015).

371. Проект по изучению рисков, связанных с деятельностью благотворительных организаций [Электронный ресурс]. – URL: http://www.un.org/ru/terrorism/ctitf/proj_charities.shtml (дата обращения 13.03.2016).

372. Терракты в Париже – объявление войны [Электронный ресурс]. – URL: <http://www.apn.ru/publications/article34327.htm> (дата обращения: 20.06.2016).

373. Финансирование терроризма // Группа разработки финансовых мер борьбы с отмыванием денег ФАТФ. [Электронный ресурс]. – URL: http://eurasiangroup.org/ru/news/typ_14.pdf (дата обращения: 24.05.2016).

374. ФСБ попросила ужесточить законы против интернет-финансирования терроризма. [Электронный ресурс]. – URL: <http://www.interfax.ru/russia/479524> (дата обращения: 24.05.2016).

375. Хакеры взломали SCADA-систему одной из американских ГЭС [Электронный ресурс]. – URL: <http://www.securitylab.ru/news/410200.php> (дата обращения: 14.04.2016).

376. Хакер выложил в сеть финансовые данные американских знаменитостей и политиков, в их числе директор ФБР [Электронный источник]. – URL: http://www.gazeta.ru/social/news/2013/03/12/n_2794737.shtml (дата обращения: 17.05.2016).

377. Цифровые информационные ресурсы [Электронный ресурс]. – URL: http://normative_reference_dictionary.academic.ru/87332/цифровые_информационные_ресурсы (дата обращения: 15.06.2016).

378. Чеченские боевики вещают на Россию из Грузии [Электронный ресурс]. – URL: <http://www.rbc.ru/politics/19/07/2001/39934.shtml> (дата обращения: 14.06.2015).

379. Что такое компьютерная сеть [Электронный ресурс]. – URL: <http://ict.edu.ru/ft/005119//ch1.pdf> (дата обращения: 19.04.2016).

380. Эксперты оценили число воюющих за «ИГ» россиян в 5 тысяч человек. 17 июня 2015 [Электронный ресурс]. – URL: <http://www.interfax.ru/russia/447922> (дата обращения: 08.08.2015).

381. Энциклопедия информационного общества [Электронный ресурс]. – URL: http://wiki.iis.ru/wiki/Информационная_среда (дата обращения: 27.05.2016).

382. Sony Pictures официально прокомментировала взлом своих серверов хакерами [Электронный ресурс]. – URL: <http://hi-news.ru/computers/sony-pictures-oficialno-prokommentirovala-vzлом-svoix-serverov-xakerami.html> (дата обращения 16.05.2016).

7. Литература на иностранных языках

383. Cassese A. Terrorism, Politics and law: The Achille Lauro Affair. – Cambridge: Polity Press, 1989.

384. Carr J. Inside cyberwarfare. Sebastopol: O' Really, 2012. 295 p.

385. Chijioke Oluocha. Internet access set to triple in Nigeria [Электронный ресурс]. – URL: <http://af.reuters.com/article/topNews/idAFJJOE75E0H920110615> (дата обращения: 27.05.2016).

386. Dawn Tay. Govt sets up cyber-security agency [Электронный ресурс]. – URL.: <http://www.asiaone.com/News/AsiaOne+News/Singapore/Story/A1Story20091001-171044.html> (дата обращения: 13.04.2016).

387. Graber P.A. Mass Media and American Politics (5-th Ed.) – Washington, 2000. P. 5-55.

388. National Advisory Committee on Criminal Justice Standards and Goals, Disorders and Terrorism. Report of the Task Force on Disorders and Terrorism. Washington, DC: U.S. Government Printing Office, – 1976. XXIV. – 580 p.

389. Post J. Differentiating the threat of chemical and biological terrorism: Motivations and constraints // Peace and Conflict: Journal of Peace Psychology. – 2002 а. – №8. – P. 186-200.

390. Siavash. Iranian Cyber Warfare Threat Assessment [Электронный ресурс]. – URL: <http://www.cyberwarzone.com/content/iranian-cyber-warfare-threat-assessment> (дата обращения: 27.05.2016).

391. Sweden has central role in cyber warfare [Электронный ресурс]. URL: <http://www.dn.se/nyheter/sverige/sweden-has-central-role-in-cyber-warfare> (дата обращения: 13.04.2016).

392. Wiener N. Cybernetics (first edition 1948). – Cambridge: MIT Press, – 1961. – 212 p.

8. Судебная практика

393. Постановление Пленума Верховного Суда РФ от 09.02.2012 №1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // Рос. газета. – 2012. – 17 февр.

394. Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // Рос. газета. – 2011. – 4 июля.

395. Постановление Пленума Верховного Суда РФ от 26.01.2010 № 1 «О применении судами гражданского законодательства, регулирующего отношения по обязательствам вследствие причинения вреда жизни или здоровью граждан» // Рос. газета. – 2010. – 5 февр.

396. Приговор № 1-262/2015 [Электронный ресурс]. – URL: <http://sudact.ru/regular/doc/Nw3su7zzqdZC/> (Дата обращения: 17.05.2016).

397. Приговор № 1-20/2015 [Электронный ресурс]. – URL: <http://sudact.ru/regular/doc/lqcdM5fJ1fLc/> (дата обращения: 17.05.2016).

398. Апелляционное определение Верховного суда РФ по делу № 16-АПУ13-3 [Электронный ресурс]. – URL: http://www.vsrp.ru/stor_pdf.php?id=540406 (дата обращения: 25.05.2016).

399. Приговор №1-248/2014 [Электронный ресурс]. – URL: <http://sudact.ru/regular/doc/2tLvc18w88N8/> (дата обращения: 25.05.2016).

400. Приговор №1-207/2010 [Электронный ресурс]. – URL: <http://sudact.ru/regular/doc/B3m6j7VeBji/> (дата обращения: 25.05.2016).

401. Приговор № 1-586/2010 [Электронный ресурс]. – URL: <https://rospravosudie.com/court-leninskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-100770808/> (дата обращения: 25.05.2016).

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

Таблица соотношения понятий «информационное пространство» и «киберпространство»

критерии разграничения	информационное пространство	киберпространство
понятие информации	информация в самом широком смысле	собственно компьютерная информация или информация, обращающаяся в Сети (Интернет или иной локальной или территориальной Сети)
понятие информационных ресурсов	документированная информация, содержащаяся в библиотеках, архивах, фондах, банках данных, информационных системах	базы данных, доступ к которым обеспечивается с помощью различных технических устройств, объединенных Сетью Интернет или иной локальной сетью
отношение к географическим и геополитическим границам	невозможность установления географических или геополитических границ	
иные характеристики		доступ к нему обеспечивается

		исключительно с помощью технических устройств, объединенных Сетью Интернет или иной локальной сетью
--	--	---

ПРИЛОЖЕНИЕ 2

Обобщающая справка об изученных уголовных делах по ст. 207 УК РФ

*В ряде приговоров предусматривалось несколько мотивов и целей совершения преступления;

Общее кол-во приговоров, изученных диссертантом, – 94.

цель – дезорганизация деятельности органов и учреждения

№	суд	подсудимый	дата вынесения приговора
1	Индустриальный районный суд г. Ижевска (Удмурдская область)	Бобков В.В. № 1-99/2014, 1-523/2013	04.04.2014
2	Первомайский районный суд г. Ижевска	Потанин С.М. № 1-286/2012	08.06.2012
3	Верховный суд Чувашской республики	Архипов И.А. № 2-51/2012	25.12.2012
4	Правобережный районный суд г. Магнитогорска Челябинской области	Сивьюк Е.В. № 1-433/2012	05.12.2012
5	Краснофлотский районный суд г. Хабаровска	Лазаренко С.В. № 1-211/2015	18.08.2015
6	Угличский районный суд Ярославской области	Григорьев В.А. №1-69/2015	08.05.2015
7	Индустриальный районный суд г. Хабаровска	*** №1-961/2015	19.11.2015
8	Фрунзенский районный суд г. Владимира	Турцев В.А. №1-183/2015	06.08.2015
9	Советский районный суд г. Казани	Назмутдинов М.А. № изъят	03.07.2015
10	Железнодорожный районный суд г. Барнаула Алтайского края	Егорова Л.В. №1-222/2015	08.05.2015

11	Камызянский районный суд Астраханской области	Евтихин А.Д. №1-75/2015	18.05.2016
12	Лихославльский районный суд Тверской области	Васильев С.Е. №1-72/2015	25.06.2015
13	Октябрьский районный суд г. Краснодара	Рогожников Я.И. №1-298/2015	19.08.2015
14	Яковлевский районный суд Белгородской области	Решетов С.А. №1-4/2016	29.01.2016
15	Ленинский районный суд г. Воронежа	Передельский В.В. №1-111/2015	07.05.2015
16	Приволжский районный суд г. Казани	Хамадьярова А.Р. №1-422/2015	09.10.2015
17	Чайковский городской суд Пермского края	Юрков А.Г. №1-45/2016	25.02.2016
18	Бердский городской суд Новосибирской области	Шинтаева Ж.С. №1-386/2015	23.12.2015
19	Ленинский районный суд г. Воронежа	Змий Д.В. №1-256/2015	22.09.2015
20	Сысертский районный суд Свердловской области	Маймулов №обезличен	30.07.2015
21	Якутский городской суд Республики Саха (Якутия)	Глега И.А. №1-212/2016	03.02.2016
22	Нурлатский районный суд Республики Татарстан	Ямщиков А.Н. №1-140/2015	25.11.2015

цель – наведение паники

№	суд	подсудимый	дата вынесения приговора
1	Индустриальный районный суд г. Ижевска (Удмурдская область)	Бобков В.В. № 1-99/2014, 1-523/2013	04.04.2014
2	Первомайский районный суд г. Ижевска	Потанин С.М. № 1-286/2012	08.06.2012
3	Угличский районный суд Ярославской области	Григорьев В.А. №1-69/2015	08.05.2015
4	Советский районный суд г. Казани	Назмутдинов М.А. №изъят	03.07.2015
5	Лихославльский районный суд Тверской области	Васильев С.Е. №1-72/2015	25.06.2016
6	Нефтекамский городской суд (Республика Башкортостан)	Сафиуллин И.Р. №1-50/2016	28.01.2016

7	Ленинский районный суд г. Воронежа	Передельский В.В. №1-111/2015	07.05.2015
8	Приволжский районный суд г. Казани	Хамадьяров А.Р. №1-422/2015	09.10.2015
9	Новомосковский городской суд Тульской области	Соболева Л.Н. №1-112/2015	30.04.2015
10	Ленинский районный суд г. Воронежа	Змий Д.В. №1-256/2015	22.09.2015
11	Мантуровский районный суд Костромской области	Киселев С.А. №1-22/2015	09.06.2015

нет указания на мотивы и цели совершенного преступления

№	суд	подсудимый	дата вынесения приговора
1	Верховный суд Кабардино-Балкарской Республики	Гилев А.С. №2-11/2014	10.07.2014
2	Мещанский районный суд г. Москвы	*** №1-403/2015	26.05.2015
3.	Кумторкалинский районный суд (Республика Дагестан)	Халимбеков А.М. №1-37/2015	27.04.2015
4	Энгельский районный суд Саратовской области	Куаншкариев А.Р. № 1-809/2015	16.12.2015
5	Приморский районный суд Санкт Петербурга	Стецюк А.Г. № 1-633/2015	12.05.2015
6	Благовещенский районный суд Алтайского края	Константинов №1-127/2012	06.06.2015
7	Красногвардейский районный суд г. Санкт-Петербурга	Попов А.О. №1-442/15	20.05.2015
8	Верецагинский районный суд Пермского края	ФИО №1-47/2015	22.04.2015
9	Невский суд города Санкт-Петербурга	Усачев М.В. №1-1038/2015	04.08.2015
10	Ишимский городской суд Тюменской области	Борисов Ю.Н. № 1-171/2015	27.07.2015
11	Советский районный суд г. Казани	Сафина Т.А. №1-471/2015	20.06.2015
12	Зареченский районный суд г. Тулы Тульской области	Траксель А.О. №1-130/2015	03.12.2015
13	Пригородный районный суд Свердловской области	Южаков М.С №1-188/2015	22.09.2015
14	Фрунзенский районный суд г. Санкт-Петербурга	*** №1-540/2015	18.06.2015

15	Центральный районный суд г. Красноярска	Орлов В.М. №1-437/2015	15.10.2015
16	Кировский районный суд г. Саратова	Владимиров С.Н. №1-323/2015	20.10.2015
17	Октябрьский районный суд г. Краснодара	Джармизе Р.Ч. №1-439/2015	17.11.2015
18	Первомайский районный суд г. Новосибирска	Шуваев А.В. №1-302/2015	09.10.2015
19	Ленинский районный суд г. Кирова	Куклин А.Л. № 1-544/2015	17.08.2015
20	Ленинский районный суд г. Кирова	Власова Т.В. №1-346/2015	19.05.2015
21	Ленинский районный суд г. Томска	Степанов Д.В. №1-578/2015	22.12.2015
21	Промышленный районный суд г. Курска	Лызенков Ю.А. №1-127/2015	12.05.2015
22	Заводской районный суд г. Кемерово	Ю. №1-786/2015	21.09.2015
23	Промышленный районный суд г. Курска	Сергеев В.В. №1-313/2015	09.09.2015
24	Ленинский районный суд г. Тамбова	Скворцов В.А. №1-119/2015	22.07.2015
25	Хостинский районный суд г. Сочи Краснодарского края	Астратенков Е.А. №1-271/2014	27.03.2016
26	Октябрьский районный суд г. Архангельска	Жимайло И.В. №1-358/2015	01.12.2015
27	Свердловский районный суд г. Костромы	Босик А.В. №1-136/2016	2.03.2016
28.	Кунгурский городской суд Пермского края	Трапезников Е.В. №1-175/2015	26.05.2015
29	Изобильненский районный суд Ставропольского края	Тяпкин В.И. №1-185/2015	07.07.2015
30	Металлургический районный суд г. Челябинска	Куоканнен В.С. №1-242/2015	28.04.2015
31	Ленинский районный суд г. Ульяновска	Селезнев П.И. №1-210/2015	28.07.2015
32	Ленинский районный суд г. Севастополь	И.Т.Ш. №1-75/2016	24.02.2016
33	Ленинский районный суд г. Тамбова	Баранов К.Г. №1-15/2016	28.01.2016
34	Волжский районный суд г. Саратова	Фарзуллаев Н.Т.о. №1-202/2015	14.10.2015
35	Прикубанский районный	Шабанов Е.А.	22.06.2015

	суд г. Краснодара	№1-532/2015	
--	-------------------	-------------	--

ЛИЧНЫЕ МОТИВЫ

№	суд	подсудимый	дата вынесения приговора
1	Благовещенский городской суд Амурской области	П. № 1-1079/2015	23.09.2015
2	Кировский районный суд г. Самары	Колесников А.А. №1-101/2016	09.02.2016
3.	Октябрьский районный суд г. Томска	Карташов В.А. №1-415/2015	23.07.2015
4	Петрозаводский городской суд Республики Карелия	Сотиков А.Л. №1-502/2015	25.06.2015
5	Нижневартовский городской суд Ханты-Мансийского автономного округа-Югра	Шумихин В.Ю. №1-1252	09.11.2015
6	Железнодорожный районный суд г. Барнаула Алтайского края	Егорова Л.В. №1-222/2015	08.05.2015
7	Хотынецкий районный суд Орловской области	Старшников Д.Н. №1-19/2015	07.05.2015
8	Центральный районный суд г. Кемерово	Дианов Е.В. №1-873/2015	29.12.2015
9	Красносельский районный суд г. Санкт-Петербурга	Круглов И.С. №1-456/2015	03.06.2015
10	Советский районный суд г. Самары	Гавриленко Е.В. №1-99/2016	09.03.2016
11	Невинномысского городского суда Ставропольского края	Манякин А.Ю. №1-154/2016	14.03.2016
12	Рубцовский городской суд Алтайского края	Солодовников С.А. №1-383/2015	20.07.2015
13	Нерюнгринский городской суд Республики Саха (Якутия)	Михайленко Р.В. №1-55/2016	02.03.2016
14	Новоильинский районный суд г. Новокузнецка	Гилагова Н.А. №1-172/2015	02.09.2015
15	Рудничный районный суд г. Кемерово	Агапов А.Г. №1-332/2015	04.08.2015
16	Нижневартовский городской суд Ханты-Мансийского автономного округа-Югра	Григорьев Ф.И. №1-646/2015	25.06.2015

17	Томский районный суд	Смокотина А.Е. №1-144/2015	09.06.2015
18	Октябрьский районный суд г. Кирова	Девярых А.В. №1-287/2015	15.06.2015

мотив – хулиганские побуждения

№	суд	подсудимый	дата вынесения приговора
1	Свердловский районный суд г. Костромы	Лаврентьева И.А. №1-340/2015	11.08.2015
2	Златоустовский городской суд (Челябинская область)	Павлов В.П. №1-592/2015	24.11.2015
3	Белорецкий межрайонный суд Республики Башкортостан	Кузнецова № 1-90/2016	02.02.2016
4	Краснофлотский районный суд г. Хабаровска	Лазаренко С.В. №1-211/2015	18.08.2015
5	Альшеевский районный суд республики Башкортостан	Исламгалиев Ф.Ф. №1-101/2015	20.05.2015
6	Угличский районный суд Ярославской области	Григорьев В.А. №1-69/2015	08.05.2015
7	Индустриальный районный суд г. Хабаровска	*** №1-961/2015	19.11.2015
8	Фрунзенский районный суд г. Владимира	Турцев В.А. №1-183/2015	06.08.2015
9	Железнодорожный районный суд г. Барнаула Алтайского края	Егорова Л.В. №1-222/2015	08.05.2015
10	Лихославльский районный суд Тверской области	Васильев С.Е. №1-72/2015	25.06.2015
11	Ленинск-Кузнецкий городской суд Кемеровской области	Филиппов В.В. №1-743/2015	17.11.2015
12	Красноурьинский городской суд Свердловской области	Вебер В.А. №1-96/2015	23.04.2015
13	Тракторозаводский районный суд г. Волгограда	Толмаков К.В. № 1-56/2016	25.01.2016
14	Советский районный суд г. Самары	Гавриленко Е.В. №1-99/2016	09.03.2016
15	Центральный районный суд г. Читы Забайкальского края	Зейнуров Е.В. №1-750/2015	18.08.2015

16	Ингодинский районный суд г. Читы Забайкальского края	Сальников Н.С. №1-99/2016	08.02.2016
17	Псковский городской суд	Гоноболев Д.Н. №1-110/2016	24.02.2016
18	Вятскополянский районный суд Кировской области	Злобин А.Ю. №1-153/2015	08.12.2015
19	Яковлевский районный суд Белгородской области	Решетов С.А. №1-4/2016	29.01.2016
20	Авиастроительный районный суд г. Казани	Фазлыев А.Т. №1-154/2013	25.11.2015
21	Черногорский городской суд Республики Хакасия	Фокин Л.А. №1-573/2015	17.12.2015
22	Засвияжский районный суд г. Ульяновска	Люкшин В.С. №1-455/2015	17.11.2015
23	Ленинский районный суд г. Воронежа	Передельский В.В. №1-111/2015	07.05.2015
24	Ленински-Кузнецкий городской суд Кемеровской области	Старков А.М. №1-583/2015	24.08.2015
25	Приволжский районный суд г. Казани	Никоноров А.Е. №1-219/2015	13.05.2015
26	Железнодорожный районный суд г. Красноярска	ФЮО №1-153/2015	27.07.2015
27	Бердский городской суд Новосибирской области	Шинтаева Ж.С. №1-386/2015	23.12.2015
28	Заринский районный суд Алтайского края	Жданов С.А. №1-17/2016	01.03.2016
29	Ленинский районный суд г. Воронежа	Змий Д.В. № 1-256/2015	22.09.2015
30	Лесосибирский городской суд Красноярского края	Сулейманов А.М. №1-310/2015	07.10.2015
31	Якутский городской суд Республики Саха (Якутия)	Глега И.А. №1-212/2016	03.02.2016
32	Чапаевский городской суд Самарской области	Попов А.А. №1-140/2015	24.06.2015
33	Солнечногорский городской суд Московской области	Новиков В.А. №1-44/2016	10.02.2016
34	Приокский районный суд г. Нижний Новгород	Лёзов В.И. №1-75/2015	06.07.2015
35	Мантуровский районный суд Костромской области	Киселев С.А. №1-22/2015	09.06.2015

ПРИЛОЖЕНИЕ 3**Диаграмма соотношения мотивов и целей совершения преступлений,
предусмотренных ст. 207 УК РФ**

*Всего исследовано 94 приговора; ряд из них предусматривал указание на несколько мотивов и целей совершения преступления



ПРИЛОЖЕНИЕ 4

Обобщающая справка об изученных уголовных делах по ст. 273 УК РФ

№	суд	подсудимый	назначенное наказание	дата вынесения приговора
1	Кировский районный суд г. Самары	Кочетков М.В. № изъят	Ч.2 ст. 146 УК РФ - 8 м. л/с; Ч.2 ст. 146 УК РФ - 8 м. л/с; Ч. 1 ст. 273 УК РФ - 1 год 4 м. л/с со штрафом 5000 р.; Ч. 1 ст. 273 УК РФ - 1 год 4 м. л/с со штрафом 5000 р.; <i>На основании ч. 2 ст. 69 УК РФ - 1 год 6 мес. л/с со штрафом 7000 р. (условно на основании ст. 73 УК РФ)</i>	31.07.2015
2	Ленинский районный суд г. Кирова	Чирков А.Н. №1-527/2015	Ч. 2 ст. 146 УК РФ - штраф 30 000 р. Ч.2 ст. 273 УК РФ - ограничение свободы 1 год. <i>На основании ч.2 ст. 69 УК РФ - 1 год ограничения свободы</i>	11.08.2015
3	Йошкар-Олинский городской суд Республики Марий Эл	Кропотов Д.А. №1-354/2015	<i>Ч.3 ст. 30 и ч.2 ст. 273 УК РФ - 1 год 6 мес. л/с (условно)</i>	26.05.2015
4	Минусинский городской суд Красноярского края	Стаченко Д.А. №1-402/2015	Ч.2 ст. 146 УК РФ - исправительные работы на 6 мес. Ч.1 ст. 273 УК РФ - 1 год л/с со	29.06.2015

			штрафом в размере 30 000 руб. <i>На основании ч.2 ст. 69 УК РФ - 1 год л/с со штрафом 30 000 руб. (условно)</i>	
5	Минусинский городской суд Красноярского края	Петров И.В. №изъят	Ч.2 ст. 146 УК РФ - исправительные работы на 6 мес. Ч. 1 ст. 273 УК РФ - 1 год л/с со штрафом 30 000 руб. <i>На основании ч. 2 ст. 69 УК РФ у год л/с со штрафом 30 000 руб. (условно)</i>	20.10.2015
6	Минусинский городской суд Красноярского края	Евтушенко Д.А. №1-384/2015	Ч.2 ст. 146 УК РФ - исправительные работы на 6 мес. Ч.1 ст. 273 УК РФ - 1 год л/с со штрафом 30 000 руб. <i>На основании ч. 2 ст. 69 УК РФ - 1 год л/с со штрафом 30 000 руб. (условно).</i>	02.06.2015
7	Черновский районный суд г. Читы Забайкальского края	Заболоцкий И.В. № 1-206/2015	Ч.2 ст. 146 УК РФ - обязательные работы на срок 200 часов; Ч.1 ст. 273 УК РФ (+ст. 64 УК РФ) - обязательные работы 400 часов. <i>На основании ч. 2 ст. 69 УК РФ - 450 часов обязательных работ.</i>	24.06.2015
8	Советский районный суд г.	Борисенко И.А.	Ч.2 ст. 146 УК РФ - 8 мес.	17.07.2015

	Томска	№1-297/2015	исправительных работ; Ч.1 ст. 272 УК РФ - 5 мес. исправительных работ; Ч.1 ст. 273 УК РФ - 1 год л/с <i>На основании ч. 2 ст. 69 УК РФ - 1 год л/с (условно).</i>	
9	Верещагинский районный суд Пермского края	Генералов К.А. № 1-2/2016, 1-219/2015	Ч.2 ст. 146 УК РФ - штраф (размер не указан); Ч.1 ст. 273 УК РФ (+ст. 64 УК РФ) - штраф (размер не указан). <i>На основании ч.2 ст. 69 УК РФ - штраф (размер не указан).</i>	11.01.2016
10	Моршанский районный суд Тамбовской области	Понкратова Н.А. №1-65/2016	Ч.1 ст. 273 УК РФ - 1 год 6 мес. л/с со штрафом 5 000 руб.; Ч.1 ст. 273 УК РФ - 1 год 6 мес. л/с со штрафом 5 000 руб. <i>На основании ч. 2 ст. 69 УК РФ - 2 года л/с со штрафом 7 000 руб. (условно)</i>	29.02.2016
11	Советский районный суд г. Томска	Дроголев А.А. №1-233/2015	Ч.2 ст. 146 УК РФ - 10 мес. л/с Ч.1 ст. 272 УК РФ - 10 мес. л/с. Ч.1 ст. 273 УК РФ - 1 год 6 мес. л/с. <i>На основании ч. 2 ст. 69 УК РФ - 1 год 8 мес. л/с (условно)</i>	24.06.2015

11	Октябрьский районный суд г. Кирова	Талимончик В.С. № 1-75/2016	Ч.2 ст. 146 УК РФ - 200 час. обязательных работ Ч.2 ст. 272 УК РФ - 10 мес. ограничения свободы; Ч.2 ст. 273 УК РФ - 1 год ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 1 год 2 мес. ограничения свободы</i>	16.02.2016
12	Октябрьский районный суд г. Владимира	Сущинин А.А. №1-268/2015	Ч.2 ст. 146 УК РФ - обязательные работы Ч.1 ст. 273 УК РФ - ограничение свободы; Ч.2 ст. 146 УК РФ - обязательные работы; Ч.1 ст. 273 УК РФ - ограничение свободы. <i>На основании ч.2 ст. 69 УК РФ - ограничение свободы</i>	23.08.2015
13	Кировский районный суд г. Томска	Тюменцев А.А. №1-196/2015	Ч.2 ст. 146 УК РФ - 1 год исправительных работ; Ч.1 ст. 272 УК РФ - 6 мес. исправительных работ; Ч.1 ст. 273 УК РФ - 1 год л/с. <i>На основании ч.2 ст. 69 УК РФ - 1 год л/с (условно)</i>	24.04.2015
14	Центральный	Химраев А.И.	Ч.2 ст. 273 УК РФ -	19.06.2015

	районный суд г. Красноярска	№1-267/2015	2 года ограничения свободы	
15	Курганский городской суд	Абросов А.А. №1-1388/2015	Ч.1 ст. 273 - 2 года ограничения свободы	21.09.2015
16	Октябрьский районный суд г. Владимира	Куркин А.С. №1-270/2015	Ч.2 ст. 146 УК РФ - обязательные работы; Ч.1 ст. 273 УК РФ - ограничение свободы; Ч.1 ст. 273 УК РФ - ограничение свободы. <i>На основании ч.2 ст. 69 УК РФ - ограничение свободы</i>	28.07.2015
17	Кировский районный суд г. Самары	Настин А.В. №1-28/2016, 1-667/2015	Ч.2 ст. 146 УК РФ - 200 час. обязательных работ; Ч.2 ст. 146 УК РФ - 200 час. обязательных работ; Ч.1 ст. 273 УК РФ - 1 год 6 мес. л/с со штрафом в размере 7000 руб.; Ч.1 ст. 273 УК РФ - 1 год 3 мес. л/с со штрафом в размере 5 000 руб. <i>На основании ч.2 ст. 69 УК РФ - 1 год 6 мес. л/с со штрафом в размере 7000 руб. (условно)</i>	12.02.2016
18	Новоуренгойский городской суд Ямало-Ненецкого автономного округа	Денисов В.П. №1-392/2015	Ч.2 ст. 273 УК РФ - 10 мес. л/с (условно)	22.12.2015

19	Центральный районный суд г. Тюмени	Пономорев В.А. №1-429/2015	Ч.2 ст. 146 УК РФ - 6 мес. исправительных работ; Ч.2 ст. 272 УК РФ - 1 год исправительных работ; Ч.1 ст. 273 УК РФ - 1 год ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 1 год ограничения свободы.</i>	4.06.2015
20	Якутский городской суд Республики Саха (Якутия)	Евстифеев О.А. №1-702/2015	Ч.2 ст. 273 УК РФ - 1 год л/с (условно)	17.07.2015
21	Таганрогский городской суд Ростовской области	Липацкий В.М. №1-64/2015, 1-709/2014	П. «в» ч.3 ст. 146 УК РФ - 1 год 6 мес. л/с; Ч.2 ст. 273 УК РФ - 1 год л/с. <i>На основании ч.3 ст. 69 - 2 года л/с (условно)</i>	03.07.2015
22	Малоярославецкий районный суд Калужской области	*** №1-62/2015	Ч.2 ст. 146 УК РФ - 1 год исправительных работ Ч.1 ст. 273 УК РФ - 1 год л/с со штрафом 30 000 руб. <i>На основании ч.2 ст. 69 УК РФ - 1 год 1 мес. л/с со штрафом 30 000 руб. (условно)</i>	29.04.2015
23	Пресненский районный суд г. Москвы	*** №1-266/2015	П. «в» ч.3 ст. 146 УК РФ - 1 год л/с со штрафом (размер не указан);	26.06.2015

			<p>Ч.1 ст. 273 УК РФ - 1 год л/с со штрафом (размер не указан).</p> <p><i>На основании ч.3 ст. 69 УК РФ - 1 год 6 мес. л/с со штрафом (размер не указан) (условно).</i></p>	
24	Октябрьский районный суд г. Кирова	Малыгин Н.Н. №1-359/2015	<p>Ч.2 ст. 146 УК РФ - 240 часов обязательных работ;</p> <p>Ч.2 ст. 272 УК РФ - ограничение свободы на срок 8 мес.;</p> <p>Ч.2 ст. 273 УК РФ - ограничение свободы на срок 10 мес.</p> <p><i>На основании ч.2 ст. 69 УК РФ - 1 год 3 мес. ограничения свободы.</i></p>	11.08.2015
25	Ленинский районный суд г. Красноярск	Путинцев В.В. №1-610/2015	<p>Ч.2 ст. 146 УК РФ - 120 часов обязательных работ;</p> <p>Ч.1 ст. 273 УК РФ - 11 мес. ограничения свободы.</p> <p>На основании ч.2 ст. 69 УК РФ - 11 мес. ограничения свободы.</p>	25.08.2015
26	Воткинский районный суд Удмуртской Республики	Красноперова О.В. №1-374/2015	<p>Ч.1 ст. 272 УК РФ - 6 мес. ограничения свободы;</p> <p>Ч.1 ст. 273 УК РФ - 1 год 4 мес. ограничения</p>	13.10.2015

			свободы. <i>На основании ч.2 ст. 69 УК РФ - ограничение свободы на срок 1 год 6 мес.</i>	
27	Первомайский районный суд г. Кирова	*** №1-169/2015	Ч.2 ст. 146 УК РФ - штраф 15 000 руб.; Ч.2 ст. 272 - ограничение свободы сроком 1 год; Ч.2 ст. 273 УК РФ - ограничение свободы сроком 1 год 6 мес. <i>На основании ч.2 ст. 69 УК РФ - ограничение свободы сроком 1 год 6 мес.</i>	17.06.2015
28	Ленинский районный суд г. Красноярск	Мишакин Е.С. №1-494/2015	Ч.2 ст. 146 УК РФ - 6 мес. исправительных работ; Ч.1 ст. 273 УК РФ - 11 мес. л/с со штрафом 5 000 руб. <i>На основании ч. 2 ст. 69 УК РФ - 1 год со штрафом 5 000 руб. (условно).</i>	09.07.2015
29	Октябрьский районный суд г. Кирова	Счастливцев М.Л. №1-526/2015	Ч.2 ст. 146 УК РФ - 240 часов обязательных работ; Ч.2 ст. 272 УК РФ - ограничение свободы сроком 8 мес.; Ч.2 ст. 273 УК РФ - ограничение свободы сроком 10 мес.	03.12.2015

			<i>На основании ч.2 ст. 69 УК РФ - ограничение свободы сроком 10 мес.</i>	
30	Ленинский районный суд г. Красноярск	Ледуховский К.В. №1-619/2015	Ч.2 ст. 146 УК РФ - 120 часов обязательных работ; Ч.1 ст. 273 УК РФ - 11 мес. ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 11 мес. ограничения свободы.</i>	22.09.2015
31	Первомайский районный суд г. Ижевска Удмуртской Республики	Галавкин С.Е. №1-215/2015	п. «в» ч.3 ст. 146 УК РФ - 1 год 6 мес. л/с; ч.2 ст. 273 УК РФ - 1 год 6 мес. л/с. <i>На основании ч.3 ст. 69 УК РФ - 2 года л/с. (условно)</i>	26.05.2015
32	Якутский городской суд Республики Саха (Якутия)	Ефимов Н.Н. №***	Ч.2 ст. 146 УК РФ - 10 мес. исправительных работ; Ч.2 ст. 273 УК РФ - 2 года л/с. <i>На основании ч.2 ст. 69 УК РФ - 2 года л/с (условно).</i>	18.06.2015
33	Минусинский городской суд Красноярского края	Булдаков С.Е. №***	П. «в» ч.3 ст. 146 УК РФ - 1 год 6 мес. л/с; Ч.1 ст. 273 УК РФ - 1 год ограничения свободы. <i>На основании ч.3 ст. 69 УК РФ - 1 год 8 мес. л/с (условно)</i>	04.08.2015
34	Элистинский	Глухов В.А.	Ч.1 ст. 272 УК РФ -	09.07.2015

	городской Республики Калмыкия	суд №1-182/2015	6 мес. ограничения свободы; Ч.2 ст. 273 УК РФ - 1 год ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 1 год 2 мес. ограничения свободы.</i>	
35	Октябрьский районный суд г. Кирова	Милютин С.В. №1-261/2015	Ч.2 ст. 146 УК РФ - 240 часов обязательных работ; Ч.2 ст. 272 УК РФ - 8 мес. ограничения свободы; Ч.2 ст. 273 УК РФ - 10 мес. ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 1 год 3 мес. ограничения свободы.</i>	03.06.2015
36	Яйский районный суд Кемеровская область	Александров П.В. №1-115/2015	Ч.2 ст. 273 УК РФ - 1 год 6 мес. л/с Ч.2 ст. 272 УК РФ - 1 год л/с <i>На основании ч.2 ст. 69 УК РФ - 2 года л/с (условно).</i>	25.12.2015
37	Октябрьский районный суд г. Красноярска	Коденко А.Е.	Ч.2 ст. 146 УК РФ - 6 мес. исправительных работ; Ч.1 ст. 273 - 8 мес. л/с со штрафом 5000 руб. <i>На основании ч.2 ст. 69 УК РФ - 8 мес. л/с со штрафом 5 000 руб. (условно).</i>	12.10.2015

38	Октябрьский районный суд г. Кирова	Поляков А.А. №1-246/2015	Ч.2 ст. 146 УК РФ - 240 часов обязательных работ; Ч.2 ст. 272 УК РФ - 8 мес. ограничения свободы; Ч.2 ст. 273 УК РФ - 10 мес. ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 1 год 3 мес. ограничения свободы.</i>	26.05.2015
39	Норильский городской суд Красноярского края	Фасхутдинов Р.К. №1-166/2015	Ч.2 ст. 146 УК РФ - 180 часов обязательных работ; Ч.2 ст. 273 - 1 год 6 мес. л/с <i>На основании ч.2 ст. 69 УК РФ - 1 год 6 мес. л/с. (условно).</i>	12.05.2015
40	Кировский районный суд г. Самары	Фадеев О.Ю. №1-152/2016	Ч.2 ст. 146 УК РФ - штраф 5 000 руб.; Ч.2 ст. 146 УК РФ - штраф 7 000 руб.; Ч.1 ст. 273 УК РФ - 2 мес. ограничения свободы; Ч.1 ст. 273 УК РФ - 2 мес. ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ 3 мес. ограничения свободы.</i>	25.03.2016
41	Октябрьский районный суд г. Кирова	Симонов Г.А. №1-345/2015	Ч.2 ст. 146 УК РФ - 300 часов обязательных работ; Ч.2 ст. 272 УК РФ -	14.08.2015

			1 год 6 мес. ограничения свободы; Ч.2 ст. 273 УК РФ - 1 год 6 мес. ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 2 года ограничения свободы.</i>	
42	Ленинский районный суд г. Иванова Ивановской области	*** №1-197/2015	Ч.2 ст. 146 УК РФ - 6 мес. л/с; Ч.2 ст. 273 УК РФ - 1 год 6 мес. л/с <i>На основании ч.2 ст. 69 УК РФ - 1 год 8 мес. л/с (условно)</i>	20.07.2015
43	Сегежский городской суд Республики Карелия	Пашков А.Н. №1-141/2015	Ч.2 ст. 146 УК РФ - 160 часов обязательных работ; Ч.2 ст. 273 УК РФ - 2 года ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 2 года ограничения свободы.</i>	10.12.2015
44	Советский районный суд г. Красноярск	Гагарин С.В. №1-549/2015	Ч.2 ст. 146 УК РФ - 9 мес. исправительных работ; Ч.1 ст. 273 - 1 год 6 мес. л/с со штрафом 10 000 руб. <i>На основании ч.2 ст. 69 УК РФ - 1 год 7 мес. л/с со штрафом 10 000 руб. (условно).</i>	05.05.2015
45	Кузьминский районный суд г.	Тулябаев А.А. №1-998/2015	Ч.2 ст. 146 УК РФ - 6 мес.	06.11.2015

	Москвы		исправительных работ; Ч.2 ст. 146 УК РФ - 6 мес. исправительных работ; Ч.2 ст. 273 УК РФ - 7 мес. л/с; Ч.2 ст. 273 УК РФ - 7 мес. л/с; Ч.2 ст. 273 УК РФ - 7 мес. л/с; <i>На основании ч.2 ст. 69 УК РФ - 1 год л/с (условно).</i>	
46	Курганский городской суд Курганской области	***	Ч.1 ст. 273 УК РФ - 2 года 6 мес. ограничения свободы; Ч.2 ст. 146 УК РФ - 420 часов обязательных работ. <i>На основании ч.2 ст. 69 УК РФ - 2 года 7 мес. ограничения свободы.</i>	23.08.2015
47	Черновский районный суд г. Читы Забайкальского края	Мазыкин А.С. №1-215/2015	Ч.2 ст. 146 УК РФ - штраф (размер не указан); Ч.1 ст. 273 УК РФ - 2 года ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 2 года ограничения свободы.</i>	30.06.2015
48	Петрозаводской городской суд Республики Карелия	Егоров О.Б. №1-429/2015	Ч.2 ст. 146 УК РФ - 300 часов обязательных работ (2 эпизода); Ч.2 ст. 273 УК РФ - 1 год ограничения	10.06.2015

			свободы (2 эпизода) <i>На основании ч.2 ст. 69 УК РФ - 1 год 1 мес. ограничения свободы.</i>	
49	Норильский городской суд Красноярского края	Зыков Д.Ю. №1-270/2015	Ч.2 ст. 146 УК РФ - 6 мес. исправительных работ; Ч.2 ст. 273 УК РФ - 1 год 6 мес. л/с. <i>На основании ч.2 ст. 69 УК РФ 1 год 7 мес. л/с (условно).</i>	28.07.2015
50	Ленинский районный суд г. Красноярска	Павлов В.И. №1-478/2015	Ч.2 ст. 146 УК РФ - 200 часов обязательных работ; Ч.1 ст. 273 УК РФ - 1 год л/с со штрафом 6 000 руб. <i>На основании ч.2 ст. 69 УК РФ - 1 год л/с. (условно).</i>	16.07.2015
51	Ачинский городской суд Красноярского края	Ершов И.А. №1-132/2015	Ч.2 ст. 146 УК РФ - 9 мес. исправительных работ; Ч.1 ст. 273 УК РФ - 10 мес. л/с со штрафом в размере 8 000 руб. <i>На основании ч.2 ст. 69 УК РФ - 1 год л/с со штрафом 8 000 руб. (условно).</i>	23.04.2015
52	Ленинский районный суд г. Кирова Кировской области	Романов А.С. №1-0393/2015	Ч.2 ст. 146 УК РФ - 20 000 руб.; Ч.2 ст. 273 УК РФ - 1 год ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 1</i>	08.06.2015

			<i>год ограничения свободы.</i>	
53	Октябрьский районный суд г. Кирова Кировской области	Поздеев В.С. №1-245/2015	Ч.2 ст. 146 УК РФ - 8 мес. исправительных работ; Ч.2 ст. 272 УК РФ - 1 год исправительных работ; Ч.2 ст. 273 УК РФ - 1 год 6 мес. ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 1 год 6 мес. ограничения свободы.</i>	13.05.2015
54	Первомайский районный суд г. Ижевска Удмуртской Республики	Савин А.А. №1-290/2015	П. в ч.3 ст. 146 УК РФ - 1 год л/с; Ч.2 ст. 273 УК РФ - 1 год л/с. <i>На основании ч.3 ст. 69 УК РФ - 1 год 1 мес. л/с (условно).</i>	17.06.2015
55	Петрозаводский городской суд Республики Карелия	Колос Г.В. №1-638/2015	Ч.2 ст. 146 УК РФ - 300 часов обязательных работ; Ч.2 ст. 273 УК РФ - 1 год ограничения свободы. <i>На основании ч.2 ст. 69 УК РФ - 1 год ограничения свободы.</i>	23.10.2015
56	Няганский городской суд Ханты-Мансийского автономного округа Югра	Шмидт А.А. №1-122/2015	Ч.2 ст. 146 УК РФ - штраф 8000 руб.; Ч.2 ст. 273 УК РФ - 1 год ограничения свободы (3 эпизода).	18.06.2015

			<i>На основании ч.2 ст. 69 УК РФ - 1 год 6 мес. ограничения свободы со штрафом 8000 руб.</i>	
57	Октябрьский районный суд г. Кирова Кировская область	Кокорин В.В. №1-418/2015	Ч.2 ст. 146 УК РФ - 240 час. обязательных работ; Ч.2 ст. 272 УК РФ - 10 мес. ограничения свободы; Ч.2 ст. 273 УК РФ - 1 год ограничения свободы <i>На основании ч.2 ст. 69 УК РФ - 1 год ограничения свободы</i>	08.10.2015
58	Центральный районный суд г. Тюмени Тюменская область	Долговых И.И. №1-673/2015	Ч.2 ст. 146 УК РФ - 200 час. обязательных работ; Ч.2 ст. 272 УК РФ - 1 год л/с; Ч.1 ст. 273 УК РФ - 1 год л/с. <i>На основании ч.2 ст. 69 УК РФ - 1 год 3 мес. л/с. (условно).</i>	05.10.2015
59	Снежинский городской суд Челябинской области	Васильев А.Н. №1-93/2015	П. в ч.3 ст. 146 УК РФ - 1 год 6 мес. л/с; Ч.2 ст. 273 УК РФ - 1 год 8 мес. ограничения свободы. <i>На основании ч.3 ст. 69 УК РФ - 2 года л/с (условно).</i>	17.09.2015
60	Ленинский районный суд г.	Обжилин А.В. №1-409/2015	ч.2 ст. 146 УК РФ - 1 год л/с	22.06.2015

Кирова Кировская область		ч.2 ст. 273 УК РФ - 2 года л/с. <i>На основании ч.2 ст. 69 УК РФ - 2 года л/с (условно).</i>	
--------------------------	--	--	--

Всего эпизодов по ст. 273 УК РФ (ч.1 и ч.2)	69
Ч.1 ст. 273 УК РФ	35
Ч.2 ст. 273 УК РФ	34

Назначение наказания по ч.1 ст. 273 УК РФ

Лишение свободы	Ограничение свободы	Другие виды наказания
19	14	Обязательные работы - 1; Штраф - 1.

Назначение наказания по ч.2 ст. 273 УК РФ

Лишение свободы	Ограничение свободы	другие
14	20	—

ПРИЛОЖЕНИЕ 5

Результаты стандартизированного интервьюирования, проводимого в целях подтверждения некоторых результатов, полученных автором в процессе написания диссертационного исследования, посвященного информационному терроризму, уголовно-правовым и иным мерам противодействия ему. (Всего приняло участие 19 чел.: из них 2 д-ра юрид. наук и 14 канд. юрид. наук по специальности 12.00.08)

1. *Какие из нижеперечисленных признаков, на Ваш взгляд, являются существенными при определении понятия терроризма?

- 1) применение насилия (9 чел. – 47%);
- 2) устрашение населения (17 чел. – 89%);
- 3) опосредованный характер воздействия (вред при терроризме причиняется одним лицам (физический, имущественных, вред государственной или муниципальной собственности), а воздействие осуществляется на других) (8 чел. – 42%);
- 4) специальная цель (10 чел. – 52,2%);
- 5) идеологическое обоснование (12 чел. – 63%);
- 6) специальные объекты воздействия (1 чел. – 5,2%);
- 7) публичность, гласность, общественный резонанс (3 чел. – 16%);
- 8) повышенная общественная опасность (5 чел. – 26%);
- 9) иной вариант ответа (0 %).

2. *Какие из нижеперечисленных признаков, на Ваш взгляд, являются существенными при определении понятия террористической деятельности?

- 1) деятельный характер (6 чел. – 31,5%);
- 2) противоправность (8 чел. – 42%);
- 3) специальная цель (9 чел. – 47%);
- 4) выражается в совершении преступлений террористической направленности (11 чел. – 59%);
- 5) организованный характер (7 чел. – 37%);
- 6) это деятельность, устрашающая население (6 чел. – 31,5%);
- 7) иной вариант ответа (1 чел. – 5,2%).

3. *Какие из нижеперечисленных признаков, на Ваш взгляд, являются существенными при определении понятия преступлений террористической направленности?

- 1) общественная опасность (8 чел. – 42%);
- 2) противоправность (7 чел. – 37%);
- 3) это деяния, связанные или способствующие достижению целей терроризма (10 чел. – 52,2%);
- 4) деяния, которые оказывают или способствуют оказанию воздействия на принятие решения или совершения действия (бездействия) органом власти, органом местного самоуправления, международной организацией, юридическим лицом, социальной группой, физическим лицом (13 чел. – 68%)
- 5) иной вариант ответа (0 %).

4. *Какие из нижеперечисленных признаков, на Ваш взгляд, могут стать отличительными и существенными при определении понятия информационного терроризма (помимо тех, что характеризуют терроризм вообще)?

- 1) платформой информационного терроризма выступает информационное пространство (11 чел. – 59%);
- 2) специальные инструменты (средства) воздействия (информация, информационные ресурсы, информационные технологии)(12 чел. – 63%);
- 3) специальный объект воздействия (сознательно-волевые компоненты личности или какой-либо социальной группы, информационные системы инфраструктуры государств, организаций, в том числе международных) (8 чел. – 42%);
- 4) специальные методы воздействия (пропаганда, дезинформация, полуправда, инсинуация и т.п.) (8 чел. – 42%);
- 5) информационный характер воздействия (6 чел. – 31,5%);
- 6) иной вариант ответа (2 чел. – 10,5 %).

5. Как Вы относитесь к выделению п. «г» в ч.2 ст. 205 УК РФ квалифицирующего признака следующего содержания: «сопряженные с посягательством на автоматизированные системы критически важных объектов и (или) потенциально опасных объектов государства, создающие опасность гибели человека, причинения значительного имущественного ущерба, аварийной ситуации, техногенной аварии, либо иных тяжких последствий, с помощью информационных технологий»

- 1) положительно, поскольку сейчас весьма актуальным является обеспечение защиты критически важных объектов и потенциально опасных объектов от подобного рода посягательств (14 чел. – 73,5%);

2) полагаю, что дифференциация ответственности за подобные деяния позволит избежать возможные посягательства в недалеком будущем (2 чел. – 10,5%);

3) считаю, что в такой дифференциации ответственности нет нужды, что обусловлено отсутствием у террористов возможности использования информационных технологий для таких целей (3 чел. – 16%)

4) иной вариант ответа (0 чел.)

6. Как Вы относитесь к изменению квалифицирующего признака, связанного с использованием информационно-телекоммуникационных сетей (в том числе сети Интернет) на «использование информационных технологий» в предлагаемом п. «г» ч.2 ст. 205 УК РФ?

1) безусловно, такие изменения необходимы, поскольку информационно-телекоммуникационная сеть является составляющей понятия информационные технологии, наравне с техническими устройствами, информационными системами и т.п., неправомерное использование которых может также спровоцировать серьезные последствия (14 чел. – 73,5%);

2) по существу такое переименование и расширение существующего в УК РФ квалифицированного признака ничего не изменит (4 чел. – 21,3%);

3) иной вариант ответа (0 чел.).

7. Согласны ли Вы с тем, что существует необходимость установления уголовной ответственности по ст. 205.2 УК РФ в том числе и за *распространение, изготовление, хранение, перевозку, ввоз на территорию Российской Федерации или вывоз с территории Российской Федерации в целях распространения материалов, призывающих к осуществлению или оправдывающих осуществление террористической деятельности?*

1) да, такая необходимость обусловлена возрастающей в последнее время опасности пропаганды террористической деятельности (13 чел. – 68%);

2) нет, в установлении дополнительной уголовной ответственности за совершение указанных действий нет необходимости (3 чел. – 16%);

3) иной вариант ответа (3 чел. – 16%).

8. Считаете ли вы чрезмерным включение в диспозицию ч. 2 ст. 280.1 (публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности РФ) понятия «электронные сети» наравне с понятием «информационно-телекоммуникационные сети»?

1) да, поскольку ни уголовному, ни специализированному законодательству неизвестно понятие «электронные сети», что может послужить возникновению проблем в правоприменительной практике (10 чел. – 52,2%);

2) да, поскольку понятие «электронные сети» входит в понятие «информационно-телекоммуникационные сети» (4 чел. – 21,3%)

3) представляется возможной и допустимой конкретизация данного понятия в исследуемом признаке для более правильной квалификации деяний (4 чел. – 21,3%);

4) иной вариант ответа (1 чел. – 5,2%).

9. Ведомство/организация, в котором/-ой Вы работаете: _____

10. Занимаемая должность (ученая степень, ученое звание):

канд. юрид. наук – 14 чел. (73,5%);

д-р юрид. наук – 2 чел. (10,5%).

БОЛЬШОЕ СПАСИБО ЗА УЧАСТИЕ В ИССЛЕДОВАНИИ!

ПРИЛОЖЕНИЕ 6

Результаты проведенного анкетирования населения «Информационный терроризм как современная угроза: общественное мнение», проводимого в целях подтверждения некоторых результатов, полученных автором в процессе исследования феномена информационного терроризма и мер противодействия данному явлению. Участвовали 167 респондентов из разных городов России.

1. Насколько, по Вашему мнению, высока вероятность информационно-технологических террористических актов? Например, разрушения системы внутренней безопасности автоматизированных систем водохранилища или электростанции, которые могут привести к гибели людей, причинения значительного имущественного ущерба, техногенной катастрофе.

а) да, я считаю, что вероятность высока (33 чел. – 20%);

б) да, я считаю в последнее время такая вероятность возросла (95 чел. – 57%);

в) нет, поскольку считаю, что совершение таких терактов в реальности невозможно (2 чел. – 1%);

г) нет, я считаю, что вероятность не высока, поскольку существует эффективная система информационной безопасности на всех критически важных объектах инфраструктуры (35 чел. – 21%);

д) иное (укажите): 2 чел. – 1 % (не задумывался).

2. Насколько, по Вашему мнению, серьезные последствия могут наступить в результате вмешательства в работу автоматизированных систем управления критически важных и (или) потенциально опасных объектов государства?

а) возможны серьезные последствия: гибель людей или причинение значительного экономического ущерба региону, вред экологии и др. (128 чел. – 77%)

б) только имущественный ущерб и нарушение нормальной работы государственных и коммерческих учреждений (**22 чел. – 13%**);

в) вероятнее всего наличие незначительных последствий в виде ущерба интересам отдельных организаций (**17 чел. – 10%**);

г) иное (укажите): **0**

3. Как, на Ваш взгляд, следует оценивать опасность распространения идеологии, присущей терроризму (лежащей в основе терроризма идеологии, оправдывающей применение насилия)?

а) высокая и всегда была таковой (**36 чел. – 21%**);

б) в последнее время возросла, в связи с активным использованием террористами новейших средств коммуникации (сети Интернет)(**118 чел. – 71%**);

в) отсутствует опасность распространения, поскольку люди понимают неправильность такого вида деятельности (**13 чел. – 8%**);

г) иное (укажите): **0**

4. Может ли распространение идеологии, присущей терроризму, преследовать цель оправдания терроризма или вовлечения в террористическую деятельность?

а) да, такая цель всегда преследуется при распространении идеологии, присущей терроризму (**105 чел. – 63%**);

б) нет, распространение идеологии, присущей терроризму, преследует только цель оправдания терроризма (**27 чел. – 16%**);

в) нет, распространение идеологии, присущей терроризму, преследует только цель вовлечения в террористическую деятельность (**13 чел. – 8%**);

г) иное (укажите): **10 чел. – 6 %** (не преследует такие цели);

12 чел. – 7 % (не исключено)

5. Насколько опасно, по Вашему мнению, распространение идеологии, присущей терроризму, в целях оправдания терроризма или вовлечения в совершение террористической деятельности?

а) да, такое распространение достойно уголовного наказания (**101 чел. – 60,5%**);

б) да, опасно при условии, что слушатели воспринимают эту информацию как оправдание терроризма или как вовлечение в совершение террористической деятельности (**40 чел. – 24%**);

в) нет, полагаю, что такой опасности нет (**26 чел. – 15,5%**).

6. Укажите, пожалуйста, Ваш пол:

а) мужской (**72 чел. – 43%**);

б) женский (**95 чел. – 57%**).

7. Ваш возраст:

- а) 18-22 лет (**41 чел. – 24,5%**);
- б) 23-45 лет (**119 чел. – 71,3%**);
- в) 45 и более лет (**7 чел. – 4,2%**)

8. Ваше социальное положение (род занятий):

- а) студент (**41 чел. – 26%**);
- б) служащий коммерческой организации (**22 чел. – 14%**);
- в) преподаватель (**25 чел. – 13%**);
- г) муниципальный служащий (**8 чел. – 4%**);
- д) сотрудник правоохранительного органа (**59 чел. – 41%**);
- е) иное (укажите)
 - пенсионер;
 - предприниматель (**12 чел. – 2%**);
 - временно-безработный;
 - военнослужащий.