Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт

кафедра международного права

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т.Ю. Сидорова
подпись инициалы, фамилия
«____» _____ 2020 г.

# БАКАЛАВРСКАЯ РАБОТА

41.03.05. Международные отношения
профиль подготовки 41.03.05.01 Международные отношения и внешняя политика

Международные инициативы в сфере борьбы с кибертерроризмом

| | | | |
|---|---|---|---|
| Руководитель | _____ | доцент, к.филос.н | М.С. Бухтояров |
| | подпись, дата | должность, ученая степень | инициалы, фамилия |
| Выпускник | _____ | | В.А. Погодаев |
| | подпись, дата | | инициалы, фамилия |

Красноярск 2020

# СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

*Актуальность темы* исследуемой проблемы заключается в том, что в силу современных процессов глобализации и цифровизации мирового сообщества, в жизнь общества и государства все больше проникают компьютерные технологии, которые затронули экономическую, технологическую, транспортную и другие сферы жизнедеятельности. Новейшие компьютерные разработки призваны облегчить нагрузку оказываемую на человечество и сделать жизнь проще и мобильнее. Однако, проникновение технологий несет за собой и угрозу того, что персональные данные многих людей могут стать общественным достоянием, производство в некоторых организациях может быть саботировано, финансовые операции могут совершаться третьими лицами, оставляя в неведении реальных владельцев денежных средств. Данный список угроз не имеет конца и с течением времени количество новых видов преступлений в цифровом пространстве будет только увеличиваться. Поэтому важно обратить внимание мирового сообщества на данную проблему и не допустить ухудшения ситуации. Только посредством совместных усилий правительства многих стран смогут дать достойный отпор такому явлению, как кибертерроризм.

*Объектом* выпускной квалификационной работы является кибертерроризм и тенденции его развития и воздействия на информационную среду, а также роль международно-правовых инициатив государств в регулировании проблемы кибертерроризма.

*Предметом* выпускной квалификационной работы являются определенные международно-правовые нормы, уставы, резолюции, соглашения и другие нормативные акты международных организаций и национальных правительств, регулирующие область киберпреступности.

*Степень научной разработанности.* При исследовании темы выпускной квалификационной работы были использованы труды таких

авторов, как: А. И. Диденко, Д. Деннинг, В. А. Мазурова, Д. Векино, М. Кенни и др. Также были использованы научно-практические журналы: “Правопорядок: история, теория, практика”; “Проблемы экономики и юридической практики”. Работа базируется на положениях Конвенции Совета Европы о киберпреступности от 23 ноября 2001 года; Концепции противодействия терроризму в Российской Федерации от 05.10.2009; Стратегической концепции НАТО от 2010 года и др.

*Цель* выпускной квалификационной работы – анализ правового регулирования кибертерроризма и международно-правовых инициатив государств, а также их действий направленных на противодействие данному явлению.

В соответствии с целью были поставлены следующие задачи:

1. Рассмотреть само понятие кибертерроризма и его роль, как фактора воздействия на международную информационную безопасность.
2. Изучить сферы сотрудничества государств и их действия по борьбе с киберпреступностью в целом и кибертерроризмом, в частности.
3. Проанализировать и сравнить международно-правовые инициативы государств по борьбе с киберпреступностью.

Структура выпускной квалификационной работы состоит из введения, двух глав, четырех параграфов, заключения и списка использованных источников.

# ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА КИБЕРТЕРРОРИЗМА

## 1.1 Понятие и особенности кибертерроризма

На современном этапе развития мирового сообщества прослеживается стремительное развитие научно-технического прогресса, который включает в себя сферу высоких технологий. В период с 2000 по 2020 годы количество пользователей сети интернет увеличилось - с 6,5 до 53,6 процентов от мирового населения. Согласно с данными Международного союза электросвязи (МСЭ) от 08.04.2020, на сегодняшний день в мире зарегистрировано 4,5 миллиарда пользователей[1]. Большая часть которых находится в развивающихся странах, что составляет около 3 миллиардов человек, а в развитых странах – 1,5 миллиард.

Таким образом, можно сделать вывод о том, что компьютерные технологии и интернет оказывают все больше влияния на нашу повседневную жизнь, однако, с другой стороны, вместе с этим возрастает количество преступлений совершаемых в сети.

Как считает, В. А. Мазуров[2]: “На данный момент, современные информационные технологии представляют собой один из важнейших факторов, оказывающих влияние на развитие общества XXI в. Они воздействуют на повседневный образ жизни людей, их образование и работу, а также, помимо этого, на взаимодействие государства и общества. Технологии в сфере информационно-коммуникационного вещания стремительно превращаются в важный стимул формирования мирового сообщества”. В то же время, с развитием научно-технического прогресса часто происходит всплеск негативного общественного поведения, которое проявляется в виде преступности. Мобильное использование современных

[1] Пользователи интернета в мире [Электронный ресурс]. - Режим доступа: https://www.internetworldstats.com/stats.htm. (дата обращения 02.04.2020).

[2] Мазуров, В. А. Кибертерроризм: понятие, проблемы противодействия / В. А. Мазуров. [Электронный ресурс] // Доклады ТУСУР. - 2010. - № 1-1. – С. 42. – Режим доступа: https://cyberleninka.ru/article/n/kiberterrorizm-ponyatie-problemy-protivodeystviya. (дата обращения: 04.04.2020).

технологий в различных сферах жизнедеятельности общества приводит к легкости нанесения вреда через сеть интернет.

По мнению А. И. Диденко[3]: “Наиболее опаснейшим преступлением связанным с компьютерными технологиями и киберпространством, является кибертерроризм. В значительной степени, это связано с влиянием компьютерной техники и интернета на повседневную жизнь людей, а также на объекты инфраструктуры. Компьютерные технологии применяются во многих областях жизни общества, начиная с больниц и заканчивая атомными электростанциями и военными объектами”.

Следовательно, можно сделать вывод о том, что государствам необходимо постоянно поддерживать безопасность компьютерной техники и телекоммуникационных сетей в сферах, оказывающих влияние на безопасность и жизнедеятельность большого количества людей.

Существуют различные толкования понятия кибертерроризм. По мнению Т. М. Шогенова[4]: “Под кибертерроризмом понимается совокупность противоправных действий, представляющих угрозу для безопасности и целостности государства и общества, деструктивные действия в отношении материальных объектов, искажение объективной информации в целях воздействия на принятие решения органами власти или международными организациями”.

Кибертерроризм является частью такого явления, как информационный терроризм. В 1980 г. данный термин был использован Б. Коллином, который на тот момент считался одним из ведущих экспертов Института Безопасности и Разведки, располагавшимся в США[5]. Используя данный термин, он попытался отметить вероятность террористических атак в

[3] Диденко, А. И. Противодействие кибертерроризму / А. И. Диденко. [Электронный ресурс] // Отечественная юриспруденция. - 2016. - № 11. – С. 23. – Режим доступа: https://cyberleninka.ru/article/n/protivodeystvie-kiberterrorizmu. (дата обращения: 05.04.2020)

[4] Шогенов, Т. М. Терроризм в условиях глобализации. Кибертерроризм / Т. М. Шогенов. [Электронный ресурс] // Социально-политические науки. - 2018. - № 3. – С. 181-182. – Режим доступа: https://cyberleninka.ru/article/n/terrorizm-v-usloviyah-globalizatsii-kiberterrorizm. (дата обращения 03.04.2020).

[5] Denning D. E. Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy [Электронный ресурс] - Georgetown University. – Режим доступа: http:// http://www.iwar.org.uk/cyberterror/resources/denning.htm. (дата обращения 03.04.2020).

киберпространстве. Развивая мысль Б. Коллина, специалисты из ФБР США дали определение кибертерроризму как действия преднамеренного характера, обусловленные политическими мотивами, включая специальные атаки на информационные компьютерные системы, компьютерные программы и данные. Однако существовала оговорка, что данные действия влекут за собой насилие направленное против гражданских лиц, либо деятельность кибертеррористов приводит к большому ущербу среди гражданского населения.

Также в национальном законодательстве США есть упоминание термина кибертерроризм. После событий, произошедших 11 сентября 2001 года в Нью-Йорке, Конгрессом США был принят федеральный закон Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act[6]. На официальном уровне документ закреплял термин кибертерроризм, а также различные формы его проявления, а именно: повреждение защищенных информационных систем с учетом ущерба, нанесенного самой сети, предназначенной обеспечивать национальную оборону и безопасность.

В Российском законодательстве термин “кибертерроризм” практически не упоминается. Вместо этого принято употреблять понятия “экстремизм” или “преступления экстремистского характера”, которые совпадают частично. Это документально подтверждено в гл. 1 Концепции противодействия терроризму в Российской Федерации от 05.10.2009 года[7]. Кроме того в Концепции имеется упоминание преступлений совершенных в сети в рамках подготовки экспертов для борьбы с терроризмом и его различными проявлениями. Также стоит отметить тот факт, что уголовное преследование связанное с совершением террористического акта

[6] Uniting and Strengthening Americaby Providing Appropriate Tools Requiredto Interceptand Obstruct Terrorism Act of 2001 [Электронный ресурс]. - Режим доступа: https://grants.nih.gov/grants/policy/select_agent/Patriot_Act_2001.pdf. (дата обращения: 09.04.2020).

[7] Концепция противодействия терроризму в Российской Федерации [Электронный ресурс] : концепция от 05.10.2009. // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_92779. (дата обращения: 25.04.2020).

предусматривается ст. 205 УК РФ, однако, в кодексе нет упоминания того, что данное преступление может быть совершенно в киберпространстве.

Также следует упомянуть, что в 2013 году Президентом РФ Путиным В. В. был издан Указ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [8], тем самым возложив на ФСБ РФ обязанности по подготовке государственной системы по обнаружению, предупреждению и ликвидации ущерба нанесенным сетевыми атаками на компьютерные ресурсы РФ.

На основе этого можно сделать вывод, что в России пока что отсутствует систематизированная правовая база по борьбе с терроризмом в информационной среде в отличии от США. Однако предпринимаются различные попытки для осуществления противодействия данному виду преступлений, но они имеют разрозненный характер. Также ощущается необходимость в создании эффективной нормативно-правовой базы. Но стоит понимать, что для более продуктивной борьбы с кибертерроризмом необходимо объединить совместные усилия многих стран.

В. Б. Вехов и С. А. Ковалев в их статье “Проблемы борьбы с кибертерроризмом”[9], утверждают следующее: “Угроза международного кибертерроризма и информационной войны является объективной реальностью XXI века, а также считается важным геополитическим фактором, который определяет направление развития современного общества. Важно отметить, что данное утверждение отражено в Руководстве по предотвращению и контролю над преступлениями, связанными с использованием сети Интернет, так, для стран, которые являются членами

[8] О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [Электронный ресурс] : Указ Президента РФ от 15.01.2013 № 31с ред. от 22.12.2017. // Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=286045&fld=134&dst=1000000001,0&rnd=0.6720959085752711#01785599082758227. (дата обращения: 25.04.2020).

[9] Вехов, В. Б. Проблемы борьбы с кибертерроризмом / В. Б. Вехов, С. А. Ковалев. [Электронный ресурс] // Правопорядок: история, теория, практика. - 2018. - № 1. – С. 91. – Режим доступа: https://cyberleninka.ru/article/n/problemy-borby-s-kiberterrorizmom. (дата обращения: 08.04.2020)

ООН данные преступные посягательства упоминаются в качестве глобальной международной проблемы".

Зарубежный исследователь Ф. Уильямс[10] определил, что кибертерроризм ярко выделяется на фоне других видов терроризма посредством среды в которой осуществляются преступления, имеющей название информационное пространство. Еще более проблематичным является то, что информационное или киберпространство постоянно развивается и расширяется по количеству пользователей, типам пользователей, точкам доступа, средствам доступа, степеням связности и формам связности. Отсюда вытекает трансграничный характер преступлений в сети и трудность установления местоположения преступников. В то же время механизмы управления сильно отстают. Следовательно, очень важно, более полно изучить природу киберпространства и виды угроз, которое оно может содержать, и диапазон возможных ответов на эти угрозы.

Угрозы, возникающие в настоящее время в киберпространстве, могут представлять риск для любого уровня безопасности (личной, коллективной и национальной) и привести к широкому спектру возможных вариантов реагирования как в физической, так и в информационной сфере взаимодействия.

Проблематика по борьбе с киберпреступностью просматривается в ст. 44-47 Стратегии национальной безопасности РФ от 31.12.2015 года[11]. В документе говорится о необходимости совершенствования правового регулирования предупреждения преступности в информационной сфере, модернизации структуры и деятельности федеральных органов исполнительной власти, развитии системы выявления, предупреждения и пресечения актов терроризма (в информационном пространстве в том числе).

[10] Williams P. Introduction. Cyberspace: malevolent actors, criminal opportunities, and strategic competition [Электронный ресурс] - Strategic Studies Institute, US Army War College. – Режим доступа: www.jstor.org/stable/resrep11980.4. (дата обращения 08.04.2020).

[11] Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента РФ от 31 декабря 2015 г. № 683 [электронный ресурс] // Справочная правовая система «ГАРАНТ». - Режим доступа: http://www.garant.ru/hotlaw/federal/688504/. (дата обращения: 25.04.2020).

Упоминаются инициативы по созданию механизмов противодействия участию граждан в деятельности террористических группировок. Особо уделяется внимание повышению общего уровня антитеррористической защищенности организаций оборонно-промышленного, ядерного, химического, топливно-энергетического комплексов страны, объектов жизнеобеспечения населения, транспортной инфраструктуры, а также иных критически важных и потенциально опасных объектов.

Таким образом, на основе сравнения работы Ф. Уильямса и Стратегии национальной безопасности РФ можно заключить, что киберпространство обладает сложной и многоуровневой структурой, которая расширяется с каждым днем и способствует трансграничному характеру преступлений, то есть противоправные действия производятся преступником не непосредственно на месте совершения теракта, а на удаленном расстоянии и через киберпространство. Именно поэтому государствам стоит акцентировать свое внимание на усилении защиты от угроз исходящих из информационной сферы и развитии международного сотрудничества по борьбе с киберпреступностью и разработке соответствующих документов.

Существуют различные трактовки определения преступлений в сети, однако, на наш взгляд, В. А. Мазуров[12] дает наиболее точное. По его мнению, к киберпреступлениям можно отнести противоправные действия, которые были совершены в киберсреде. Сюда включаются: намеренное нарушение работы компьютеров, программного обеспечения, локальных сетей, осуществление внесения изменений в базы данных без разрешения организаций, а также другие преступления для совершения которых использовался персональный компьютер, либо иной вредоносный компьютерный софт. Данным образом автор обобщил основные виды и

[12] Мазуров, В. А. Кибертерроризм: понятие, проблемы противодействия / В. А. Мазуров. [Электронный ресурс] // Доклады ТУСУР. - 2010. - №1-1. – С. 44. – Режим доступа: https://cyberleninka.ru/article/n/kiberterrorizm-ponyatie-problemy-protivodeystviya. (дата обращения: 08.04.2020).

способы совершения преступлений в информационной среде, а также указал объекты находящиеся в зоне риска.

Среди западных исследователей в сфере информационных преступлений стоит отметить определение кибертерроризма, данное Д. Деннинг[13]. По ее мнению, кибертерроризм - это процесс сближения терроризма, в его классическом понимании, и киберпространства. Под данным явлением обычно подразумеваются незаконные нападения или угрозы нападения на компьютеры, информационные сети и хранящуюся в них информацию, совершающиеся с целью запугивания или принуждения правительства для достижения политических, а также социальных целей преследуемых террористической организацией. Кроме этого, автор считает, что для того, чтобы квалифицировать атаку в качестве акта кибертерроризма, она должна привести к насилию в отношении людей, имущества или, по крайней мере, причинить достаточный ущерб, чтобы вызвать страх. Серьезные атаки на критически важные объекты инфраструктуры государства могут считаться актами кибертерроризма, в зависимости от их воздействия. Если последствием атаки является нарушение работы несущественных секторов инфраструктуры, то она не может рассматриваться, как одно из проявлений кибертерроризма.

Исходя из данного определения можно сделать вывод, что обычно для понимания сущности кибертерроризма, некоторые исследователи оперируют ситуациями, где атака направлена исключительно против компьютеров, информационных сетей и хранящейся в них информации. Однако, стоит понимать, что акт кибертерроризма считается свершенным не только тогда, когда атака была направлена против компьютерных систем, но и тогда, когда многие другие факторы и возможности виртуального мира были использованы преступником для достижения своей цели, какой бы она ни была. Также можно отметить, что данное определение очень отличается от

[13] Denning D. E. “Cyberterrorism”, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services [Электронный ресурс] - US House of Representatives. – Режим доступа: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. (дата обращения 08.04.2020).

распространенных точек зрения, которые используют СМИ и широкая общественность.

На основе сравнения двух определений кибертерроризма данных В. А. Мазуровым и Д, Деннинг можно отметить основное сходство точек зрения авторов в вопросе того где совершаются киберпреступления и против чего они направлены. Однако, стоит учесть тот факт, что определение Д. Деннинг в большей мере раскрывает сущность вопроса и дает взглянуть значительно шире на исследуемую тему.

Чаще всего, термин «кибертеракт» используется для обозначения действий связанных с нарушением работы информационных систем, оказывающих устрашающий эффект на общество, причинением ущерба имуществу либо наступлением иных тяжких последствий, с целью повлиять на работу и принимаемые решения государственных органов власти или международных организаций.

По словам Ю. В. Гаврилова[14]: “Кибертеракт представляет серьезную угрозу для всего человечества, сравнимой с ядерным, бактериологическим и химическим видами вооружений. Данный вид преступлений не имеет государственных границ, а лица их совершаемые способны представлять равную угрозу для информационных систем, которые расположены практически в любой точке мира. Процесс обнаружения и нейтрализации кибертеррориста очень осложнен из-за наличия малого количества следов остающихся после преступника и их виртуальной специфики”.

Карамова Э. И. и Фомин С. М. в своей статье “К вопросу о кибертерроризме в глобализирующемся мире”[15], утверждают следующее: “Всевозможными способами кибертеракт может вывести из рабочего состояния информационные инфраструктуры государств, что, в свою

[14] Гаврилов, Ю. В. Современный терроризм: сущность, типология, проблемы противодействия / Ю. В. Гаврилов, Л. В. Смирнов. – Москва : ЮИ МВД РФ, 2003. – С. 24-26.

[15] Карамова, Э. И. К вопросу о кибертерроризме в глобализирующемся мире / Э. И. Карамова, С. М. Фомин. [Электронный ресурс] // Социально-политические науки. - 2016. - № 3. – С. 154. – Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-v-globaliziruyuschemsya-mire. (дата обращения: 20.04.2020).

очередь, может привести к катастрофическим последствиям для них. Основой для проведения кибертеракторов являются страны, лидирующие в области высоких технологий и спутниковой связи, а также глобальных сетей. Кибертеракт является угрозой для главных элементов инфраструктуры каждой страны”.

Также Карамова Э. И. и Фомин С. М. выделяют основные элементы инфраструктуры на которые кибертеррористы совершают нападения и последствия данных атак:

1. Электричество: совершение атаки на систему через которую совершается управление с помощью беспроводных модемов или интернет соединений может временно отключить локальное электропитание;

2. Транспорт: преступник может получить доступ над контролем системами управления железнодорожных путей;

3. Водные ресурсы: путем атаки на систему управления через Интернет возможно повысить содержание хлора и других химических веществ;

4. Энергетика: временное отключение источников энергии;

5. Финансы: последствием атаки может стать закрытие финансового рынка с помощью выведения серверов из строя, посредством внедрения сетевого червя;

6. Информационные технологии: при помощи наличия уязвимостей в программном обеспечении преступники имеют возможность получить доступ к критическим системам, что может повлечь за собой различные атаки на другие элементы, которые имеются в информационной инфраструктуре, а также создать расширенные проблемы со связью в сети интернет.

Вышеперечисленные элементы инфраструктуры являются необходимыми составляющими для нормального обеспечения жизнедеятельности любого государства. Следовательно, первоочередной задачей каждой страны является создание надежной информационной системы защиты соответствующих жизненно важных “артерий”. На фоне

набирающего с каждым днем темп научно-технического прогресса и цифровизации различных систем жизнеобеспечения государства не следует забывать о их защите от киберугроз, а рассматривать этот вопрос на высшем уровне для успешного проведения в жизнь политики национальной безопасности.

С. Ю. Асеев[16] подчеркивает интересную особенность: “Кибертеррористы помимо совершения террористических актов при помощи электронных сетей, также обладают возможностью получать доступ к конфиденциальной информации, государственной тайне. Многие сайты государственных органов власти содержат информацию различной степени важности. К примеру, схемы подземных коммуникаций, строящиеся стратегические объекты, места расположения объектов жизнеобеспечения. Более того, преступники могут иметь доступ к личным данным многих пользователей сети, от адреса и номера телефона до подробной информацией о личности”.

Таким образом, под кибертеррористические атаки в теории подпадают преступления кибертеррористов, приводящие, к примеру, к трудностям в экономической сфере или отключению электроэнергии, водоснабжения и пр.

Рассмотрев понятие и основные особенности кибертерроризма можно заключить, что развитие современных информационных технологий во всем мире является предпосылкой распространения кибертерроризма. Они оказывают все большее влияние на нашу жизнь и безопасность. Однако, пока что не существует систем, которые можно с уверенностью назвать неуязвимыми для преступников. Это прежде всего связано с отсутствием систематизированной правовой базы в сфере борьбы с кибертерроризмом, а также с низким уровнем защиты сетевых ресурсов различных организаций, предприятий и трансграничным характером преступлений. Угроза кибертерроризма остается весьма значимой для всего мирового сообщества,

[16] Асеев, С. Ю. Проблема определения кибертерроризма / С. Ю. Асеев, В. А. Воронцов. [Электронный ресурс] // Общество и цивилизация. - 2016. - № 2. - С. 49-53. – Режим доступа: https://www.elibrary.ru/item.asp?id=26399093. (дата обращения: 10.04.2020).

наравне с иными глобальными проблемами и в ближайшем перспективе имеет шанс выйти на одно из первых мест в связи с компьютеризацией многих отраслей нашей повседневной жизни.

## 1.2 Воздействие кибертерроризма на международную информационную безопасность

По прошествии каждого года можно наблюдать стремительно увеличивающееся количество разновидностей террористической активности, охватывающей и интегрирующейся в национальные, религиозные и этнические конфликты. На фоне процессов глобализации в современном мире терроризм приобретает форму самостоятельной движущей силы, способной стать противовесом государственной целостности многих государств.

В современном мире возрастает устрашающая роль террористических организаций и открываются новые возможности для совершения преступлений. В связи с этим, Т. М. Шогенов[17] утверждает, что: “Уровень воздействия оказываемого терроризмом на устройство внутренней политики некоторых стран, и на международную стабильность в общем увеличивается в быстрых темпах, также отмечается активное развитие преступности с применением современных компьютерных систем”.

Также автор выделяет основные приемы и способы, которые используют преступники при совершении кибертеррактов в сети:

- создание и внедрение вирусных программ, которые выводят технику из строя;
- кража, удаление информационных компьютерных ресурсов, имеющих стратегическое значение для государства;
- запугивание путем угрозы опубликовать конфиденциальную информацию;

[17] Шогенов, Т. М. Терроризм в условиях глобализации. Кибертерроризм / Т. М. Шогенов. [Электронный ресурс] // Социально-политические науки. - 2018. - № 3. – С. 181-182. – Режим доступа: https://cyberleninka.ru/article/n/terrorizm-v-usloviyah-globalizatsii-kiberterrorizm. (дата обращения 09.04.2020).

- распространение фэйковой информации с целью расколоть общество, а также распространение пропагандистских материалов экстремистского характера посредством получения контроля над телекоммуникационными каналами вещания.

Т. М. Шогенов подчеркивает, что данные приемы и способы имеют широкое распространение и развиваются параллельно с защитными программами, которые применяются разработчиками различных сетей.

В иностранных источниках представленных М. Кенни[18] и Отчетом международного института по борьбе с терроризмом от 24 апреля 2017 года[19] отмечается, что киберпреступность охватывает широкий круг видов деятельности, для которых компьютер является средством совершения преступления. В основном автор включает сюда:

- слежку и преследование представителей власти, а также представителей военных и частных структур;
- шпионские атаки, кража личных данных и корпоративный шпионаж с целью вымогательства, совершающиеся отдельными небольшими группами преступников, а не террористическими организациями в их традиционном понимании;
- атаку критически важных объектов инфраструктуры, включая объекты электроэнергетики, атомной энергетики и авиации;
- подмену документов в базах данных, государств и частных организаций;
- осуществление тайных кибератак на внешнеполитические институты, государственные органы и дипломатические объекты с помощью вирусных программ, которые помогают взять под контроль атакуемую систему, общаться с удаленными серверами, загружать файлы и выполнять команды.

[18] Kenney M. Cyberterrorism in a post-stuxnet world [Электронный ресурс] - Strategic Studies Institute, US Army War College. – Режим доступа: www.jstor.org/stable/resrep11980.9. (дата обращения 09.04.2020).
[19] International Institute for Counter-Terrorism (ICT). Cyber Report 24 September-November 2017 [Электронный ресурс]. – Режим доступа: www.jstor.org/stable/resrep17687.7. (дата обращения 09.04.2020).

В своих работах отечественный и зарубежный исследователи отразили основные способы совершения киберпреступлений террористами, которые практически идентичны, за исключением, информации о слежке и шпионских атаках представленной в работе М. Кенни, что позволяет расширить перечень угроз представляемых кибертерроризмом.

Важно упомянуть, что глобальная сеть является и будет оставаться одним из популярнейших ресурсов с помощью которого кибертеррористы осуществляют свои преступления, невзирая на меры, которые предпринимаются властями и подконтрольными им службами и органами.

Глобализация современного общества является главным фактором из-за которого кибератаки имеют возможность превратиться в опаснейший инструмент в арсенале террористических организаций и для более оперативного противостояния всевозможным кибератакам, совершаемым обычно на трансграничном уровне следует создать систему взаимодействия важнейших национальных органов, которые отвечают за безопасность в сети.

Более того стоит подчеркнуть, что на сегодняшний день происходит процесс создания системы международной информационной безопасности, призванной создать условия для более эффективного противодействия угрозам стратегической стабильности и благоприятствовать равноправному сотрудничеству в глобальном информационном поле.

Е. С. Пелевина, в своей статье “Информационные угрозы кибертерроризма”[20], отмечает: “Преступные элементы, использующие новейшие разработки в сфере информационно-коммуникационных технологий представляют большую угрозу. Их деятельность коренным образом меняет способы того, как террористические организации ведут свою деятельность. Данные организации имеют многоуровневую структуру, в которую входят различные группы, имеющие своих лидеров. Кроме того они способны объединять свои усилия для достижения общих целей. Условием

[20] Пелевина, Е. С. Информационные угрозы кибертерроризма / Е. С. Пелевина. [Электронный ресурс] // Евразийский Союз Ученых. - 2015. - № 11-2. – С. 101. – Режим доступа: https://cyberleninka.ru/article/n/informatsionnye-ugrozy-kiberterrorizma. (дата обращения: 11.04.2020).

существования данных структур является информационно развитая среда. Одной из их главных особенностей считается способность быстро адаптироваться к изменяющимся условиям в политической жизни общества".

Действительно, нельзя не согласиться со словами автора, раскрывающей проблематику распространения информационных технологий и их применения кибертеррористами. Технологическое развитие стало одной из причин появления трансграничного характера преступлений, создания террористических структур в сети, что лишь усложнило борьбу с преступностью в компьютерной среде и внесло новые корректировки в международную повестку дня.

Также Е. С. Пелевина говорит о том, что для нарушения работы информационных систем, преступники чаще всего прибегают к хакерским атакам цель которых на время вывести из строя определенные сервисы и службы в сети интернет, контролирующие информационный поток. Данные атаки чаще всего совершают так называемые «временные террористы» - частные лица, не связанные прямым образом с террористическими организациями, но разделяющие в некоторой степени их идеи.

По мнению того же автора, данные лица имеют множество средств, с помощью которых они могут нарушить или остановить работу различных серверов. К примеру, во время конфликта в Косово, хакеры из Белграда проводили атаки на сервера НАТО. С помощью большого количества команд, проверяющих работу серверов и их подключение к интернету они успешно перегружали систему. Также в качестве средства выражения своего возмущения происходящему они прибегали к бомбардировкам электронных адресов политиков. Они одновременно засыпали их адреса тысячами сообщений, используя автоматизированные команды, и в результате данных действий происходила блокировка их электронных адресов, временно приостанавливая работу данного канала связи. Американскими СМИ было отмечено, что конфликт в Косово положил начало становления

киберпространства, как зоны, где военные действия ведутся путем хакерских атак.

Кроме того, А. А. Галушкин[21] поднимает проблему анонимного предоставления услуг связи. По его мнению, подавляющее количество людей в наше время используют услуги крупных провайдеров, которые осуществляют свою деятельность по передаче данных в открытом и официальном формате, однако, невзирая на это, существует немалое количество организаций, которые предоставляют свои услуги на условиях полной анонимности.

К данной категории организаций он относит зарубежные дата-центры, хостинг-компании и интернет-провайдеров, на официальном уровне предоставляющие услуги по создания анонимного канала связи и выделения специальных виртуальных серверов. Их клиенты имеют полную анонимность, однако, в случае правонарушения фактически могут избежать наказания за свои действия.

Исходя из этого, стоит отдавать себе отчет о том, что те, кто имеет доступ к данным технологиям и злой умысел, могут использовать их для маскировки или сокрытия своей личности и своего реального местоположения, чтобы избежать преследования за совершенные преступления. Что тоже важно учитывать при борьбе с правонарушениями в данной сфере. Также стоит задуматься о создании мер, защищающих доступ к данным услугам связи от кибертеррористов.

Другой проблемой являются актуальные методики в области коммуникаций, такие как: социальные сети, интернет-пропаганда и прочие. Они предоставляют возможность преступникам расширить число своих последователей в сети, производить вербовку новых сторонников и распространять пропагандистские материалы.

[21] Галушкин, А. А. К вопросу о кибертерроризме и киберпреступности / А. А. Галушкин. [Электронный ресурс] // Вестник РУДН. Серия: Юридические науки. - 2014. - № 2. – С. 46. – Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-i-kiberprestupnosti. (дата обращения: 17.04.2020).

Современные сервисы в области информационных коммуникаций открывают широкий простор и новые возможности для работы террористических организаций. Е. А. Кошечкина[22] считает, что на данный момент злоумышленники с помощью сети интернет имеют возможность с легкостью создавать сообщества лиц, которые в ближайшем будущем могут непосредственно стать участниками террористического акта. Однако, сами организаторы преступления могут так и остаться неизвестными. В качестве примера можно привести деятельность запрещенной в большинстве государств мира террористическую организацию Исламское государство (ИГИЛ). В последние годы новые последователи данной террористической организации вербуются в сети интернет.

Активизацию деятельности кибертеррористов в этой сфере автор связывает с тем, что данный способ по привлечению сторонников практически не требует вливания больших денежных средств для проведения и подготовки террористических актов. Потому что для совершения кибератаки или формирования и управления действиями отдельных террористических ячеек преступникам необходимо иметь всего лишь одно устройство с доступом в интернет. Простые способы осуществления кибертеррактов, а также трудность установления причастности лиц к совершению преступлений остаются главными причинами стремительного развития кибертерроризма.

Л. А. Бураева в своей статье “Кибертерроризм в молодежной среде”[23] отмечает, что социальные сети и мессенджеры представляют интерес для террористических организаций по одной очень простой причине. И это связано не только с легкостью общения в любой точке мира, но и с возможностью работать по различным направлениям, воздействуя, точечно на определенную аудиторию, или охватывая более широкие массы. В данном

[22] Кошечкина, Е. А. К вопросу о проблемах противодействия кибертерроризму / Е. А. Кошечкина. // ОНВ. ОИС. - 2017. - № 4. – С. 100.

[23] Бураева, Л. А. Кибертерроризм в молодежной среде / Л. А. Бураева. [Электронный ресурс] // Проблемы экономики и юридической практики. - 2016. - № 2. – С. 273. – Режим доступа: https://www.elibrary.ru/item.asp?id=25903441. (дата обращения: 18.04.2020)

случае в повышенную группу риска входит молодежь. Кибертеррористам проще войти в доверие к молодым людям, так как в их социальных сетях имеются личные данные, интересы, что упрощает террористам задачу по точечному воздействию, рассчитанному на определенную группу населения. Более того, молодые несовершеннолетние люди еще с неустойчивой психикой проще подвергаются внушению. Следовательно, пропаганду идей террористического и экстремистского характера нацеленную на молодежь, проще совершать посредством социальных сетей.

Пропагандирование расовой, религиозной, а также иных проявлений нетерпимости имеет разрушительные последствия для несформировавшихся молодых умов. С каждым днем молодые люди, используя интернет и социальные сети, получают все больше информации не отдавая себе отчет в том, они могут стать жертвами радикальных религиозных течений. Под влиянием террористических организаций у молодежи происходит подмена ценностей. Они верят в то, что смогут очистить страну от проблем, однако, им не сразу приходит осознание того, что путь, который они выбрали для этого является недопустимым.

Также об активности террористов в сфере пропаганды пишет М. Кенни[24], по его мнению для большей эффективности, террористам необходимо донести свои идеи до широкой аудитории, и они часто используют для этого средства массовой информации и интернет. Чтобы повысить пропагандистскую ценность своих сообщений, террористы и их сторонники часто раздувают свою способность осуществлять разрушительные атаки, будь то с использованием химического, биологического, ядерного оружия.

Если смотреть на вещи реально, то обычно существует большой разрыв между заявленными террористами желаниями и их технологическими

[24] Kenney M. Cyberterrorism in a post-stuxnet world [Электронный ресурс] - Strategic Studies Institute, US Army War College. – Режим доступа: www.jstor.org/stable/resrep11980.9. (дата обращения 19.04.2020).

возможностями по воплощению пропагандистских высказываний в реальность.

Какова бы ни была пропагандистская ценность заявлений террористов, их тонко завуалированные угрозы редко воплощаются в жизнь. Ни террористическая сеть, ни хакеры, действующие от имени террористических организаций, не приблизились к осуществлению кибератак, способных вызвать большой экономический и политический коллапс.

Хотя некоторые террористические веб-сайты и дискуссионные форумы содержат информацию и программное обеспечение для базового взлома, нет никаких доказательств того, что боевики имеют доступ к лабораториям со специализированным программным обеспечением и оборудованием, необходимым для осуществления таких атак.

М. Кенни считает, что на данный момент террористы продолжают использовать интернет для сбора информации, распространения пропаганды, радикализации своих сторонников и координации своей деятельности, включая проведение более простых атак из плоти и крови с использованием обычных вооружений. Многие террористические группировки по-прежнему предпочитают кустарно изготовленные взрывные устройства информационным атакам. Таким образом кибертерроризм остается гипотетической угрозой, даже если общий уровень угрозы в киберпространстве увеличился.

Проанализировав исследования Л. А. Бураевой и М. Кенни можно увидеть две различные позиции по данному вопросу. Отечественный исследователь видит прямую угрозу в деятельности террористов по привлечению новых сторонников посредством пропаганды и действиях, которые они грозятся совершить. Исходя из этого можно заключить, что в этой связи правоохранительным органам многих государств следует усилить меры по противодействию распространения в социальных сетях пропагандистских материалов. Создать системы по вычислению

пользователей, входящих в группу риска и склонных попасть под влияние преступных элементов.

Однако М. Кенни считает пропаганду и действия террористов в киберпространстве неубедительными и аргументирует это мало развитой ресурсной базой для воплощения этих замыслов в жизнь, но и не отрицает угрозы данных заявлений. Нельзя не согласиться с его точкой зрения насчет того, что по сей день террористы предпочитают сеять страх и панику с помощью проведения обычных атак в людных местах. Следовательно можно сделать вывод о том, что кибертерроризм является мнимой угрозой, но отвергать его реальный потенциал недопустимо и следует предотвратить возможность реализации данных намерений в жизни.

Деятельность террористических группировок в сети интернет весьма успешна. Согласно исследованиям Национального антитеррористического комитета России в 2016 г. в стране было обнаружено около 30 тысяч сетевых ресурсов экстремистской и террористической направленности.

Ранее упомянутый ИГИЛ к сегодняшнему дню имеет ряд медийных компаний, сумевших привлечь немалое количество зрителей. Изначально Исламское государство снимало ролики низкого качества, но благодаря развитию цифровых технологий они сумели проникнуть во многие популярные интернет-ресурсы и создать свои сайты с содержанием экстремистского характера. Одной из особенностей их деятельности является то, что у террористической организации отсутствует единый центр по работе с медиа-ресурсами. В их распоряжении имеется множество независимых друг от друга медиа-групп, чья деятельность распространяется на территориях: от Африки до Северного Кавказа.

Л. А. Бураева в своей работе “Мировой опыт противодействия экстремизму и терроризму в глобальном информационном пространстве”[25],

[25] Бураева, Л. А. Мировой опыт противодействия экстремизму и терроризму в глобальном информационном пространстве / Л. А. Бураева. [Электронный ресурс] // Теория и практика общественного развития. - 2015. - № 18. - С. 134. – Режим доступа: https://cyberleninka.ru/article/n/mirovoy-opyt-protivodeystviya-ekstremizmu-i-terrorizmu-v-globalnom-informatsionnom-prostranstve. (дата обращения: 18.04.2020).

отмечает, что современные террористические организации активно следят за новейшими тенденциями в информационной сфере. Их нынешние проекты содержат меньше сцен жестокости и насилия, а в большой степени пропагандируют повышение уровня жизни населения, развитие экономической, культурной сфер при условии, что данные организации будут находится у власти. Цель данной пропаганды заключается в убеждении новой аудитории в стабильности развития данных организаций.

В этой сфере автор выделяет запрещенную на территории большинства стран террористическую организацию ИГИЛ. Террористическая организация является максимально открытой и отражает такой современный тренд, как открытость и гласность информации. Они отказались от форумов с ограниченным доступом на арабском языке и теперь в открытую через известнейшие информационные ресурсы осуществляют свои деятельность.

Обобщая вышесказанное можно заключить, что борьба властей различных государств с данным феноменом требует больших усилий и лучших результатов. Властям следует полностью пересмотреть свой подход к работе, так как террористические элементы проявляют большую креативность и тем самым обладают большим преимуществом.

В. А. Мазуров[26] отмечает: “Террористический акт в информационном пространстве имеет различия в форме оказания влияния на киберпространство, исходя из своих целей, которые остаются характерными для политического террористического акта. Следует различать тактику и приемы кибертерроризма, которые во многом разняться с тактикой ведения информационной войны. Главным в тактике кибертерроризма является результат террористического акта. Он должен иметь ощутимые серьезные последствия и получить большую огласку среди населения, вызвав тем самым общественный резонанс”.

[26] Мазуров, В. А. Кибертерроризм: понятие, проблемы противодействия / В. А. Мазуров. [Электронный ресурс] // Доклады ТУСУР. - 2010. - №1-1. – С. 45. – Режим доступа: https://cyberleninka.ru/article/n/kiberterrorizm-ponyatie-problemy-protivodeystviya. (дата обращения: 18.04.2020).

Основной целью кибертеракtов является вывод из рабочего состояния информационно-технологической части инфраструктуры государства или применение данной инфраструктуры для создания условий, которые могут привести к трагическим последствиям внутри общества и государства. Стоит отметить, что количество актов кибертерроризма напрямую зависит от уровня развития информационной инфраструктуры государства.

Кибератаки позволяют преступникам проникнуть в систему на которую совершается нападение и получить над ней контроль, а также глушить средства обмена информацией и производить другие разрушительные действия.

Кибератаки высокого уровня автор разделяет на две главные категории:

- вывод из строя информационных систем. Атаки данной категории получили наибольшее распространение, их основной принцип действия направлен на временное выведение из рабочего состояния определенных систем отвечающих за управление и контроль над потоком информации. Результатом данных действий является нарушения работы объекта нападения, который начинает бесконтрольно функционировать, что представляет большую опасность для производств в атомной, химической и военной отраслях;

- разрушительные атаки. Их основной целью являются объекты информационных систем. Данный вид атак может привести к уничтожению информационных ресурсов, линий передачи информации. В случае, если одна из систем участвует в управлении критических инфраструктур государства, то велик риск возникновения последствий по масштабу сопоставимых с обычными актами терроризма, которые осуществляются посредством взрыва.

Достижения в научно-технической сфере, ускорившие процесс глобализации, а также повышения уровня жизни в мире являются средствами с помощью которых отдельные лица или группировки могут совершить

преступления. Кибертеррористический акт может стать причиной массовой дезорганизации. На сегодняшний день действия кибертеррористов могут оказать больший ущерб, в отличии от обычных взрывных устройств. Террористы стали иметь доступ к средствам, позволяющим нанести огромный ущерб компьютерным системам и другим электронным устройствам.

Соединение технологического и научного потенциала развитых стран и особенно в России, представляет на данный момент большую угрозу мировым информационным системам. Кроме того, стоит упомянуть, что ситуация значительно усложняется из-за нормативно-правовой базы, на сегодняшний день не способной дать серьезный ответ сложившейся угрозе. На данный момент практически любая существующая террористическая организация имеет возможность совершить кибертеракт.

Подводя итог можно с уверенностью сказать, что теракты с применением высоких достижений технологической отрасли нового столетия могут стать причиной системного кризиса всего мирового сообщества и стать масштабной угрозой для нормального существования некоторых регионов мира, что обычно не является характерным для классических террористических актов.

# ГЛАВА 2. ИНИЦИАТИВЫ ГОСУДАРСТВ МИРА ПО БОРЬБЕ С КИБЕРТЕРРОРИЗМОМ

## 2.1 Международное сотрудничество в борьбе с киберпреступностью

Киберпреступность продолжает расти несмотря на продолжающиеся усилия по исправлению положения в государстве и на международном уровне. Легкость доступа к осуществлению киберпреступной деятельности, находясь за пределами границ государств, делает эту проблему международной. Изучение схем сотрудничества, используемых в межправительственных учреждениях, позволяет выявить возможные условия, побуждающие государства к сотрудничеству в борьбе с киберпреступностью. Проверка этих условий показывает, что успешность раннего упреждения в соответствующей проблемной области служит самым мощным стимулом сотрудничества в рамках международных институтов по борьбе с киберпреступностью.

Американский исследователь в сфере кибертерроризма Джобел Векино[27] отмечает, что проблема киберпреступности продолжает расти на международном уровне. По его оценкам, она будет стоить предприятиям по всему миру в среднем 6 миллиардов долларов в год до 2021 года. Некоторые государства обладают большими возможностями для борьбы с киберпреступностью, чем другие. В некоторых случаях многонациональные корпорации и научно-исследовательские институты обладают более мощными возможностями по смягчению последствий киберпреступности, чем некоторые государства. Повсеместный характер киберпреступности также создает трудности для любого государства в борьбе с киберпреступниками в одиночку.

[27] Vecino J. United by Necessity: Conditions for Institutional Cooperation against Cybercrime [Электронный ресурс] - The Cyber Defense Review. – Режим доступа: www.jstor.org/stable/26846124. (дата обращения 16.04.2020).

В этой связи, хотелось бы отметить деятельность НАТО по противодействию распространению кибертерроризма.

Для определения угроз кибертерроризма в рамках организации была создана новая версия Стратегической концепции НАТО, подписанная в Лиссабоне в 2010 году[28]. В документе атаки на компьютерные системы отмечены как действия представляющие большую опасность для безопасности и развития государств-членов организации. Данная угроза отражается в документе наравне с такими проблемами как распространение оружия массового поражения и терроризмом в его классическом проявлении.

Также стоит отметить, что согласно Стратегической концепции НАТО, состоянием безопасности в киберпространстве считается поддержание постоянной готовности к отражению потенциальных угроз, число которых возрастает с каждым днем, и реализация ответных действий направленных на их подавление.

По мнению отечественного исследователя А. В. Казаковцева[29], одним из важнейших шагов по обеспечению кибербезопасности в рамках организации считается принятие Официальной политики НАТО в сфере обороны в киберпространстве в 2008 г. В документе автором подчеркивается пункт об оказании помощи в борьбе с компьютерными атаками союзникам Альянса, по их непосредственному запросу.

К 2014 году была утверждена новая версия политики НАТО в сфере обороны в киберпространстве. В рамках этой политики признается, что защита в киберпространстве входит в число основных задач НАТО по обеспечению коллективной обороны союзников. Однако, стоит отметить, что к более полному содержанию данных документов доступ имеет ограниченный круг лиц в рамках организации.

[28] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation. Active Engagement, Modern Defence of 2010 [Электронный ресурс]. - Режим доступа: https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf. (дата обращения: 17.04.2020).

[29] Казаковцев, А. В. НАТО и кибербезопасность / А. В. Казаковцев. [Электронный ресурс] // Вестник ВолГУ. История. Регионоведение. Международные отношения. - 2012. - № 2. – С. 111. – Режим доступа: https://cyberleninka.ru/article/n/nato-i-kiberbezopasnost. (дата обращения: 24.04.2020).

С тех пор обновленный план действий был одобрен союзниками в феврале 2017 года. Эта политика устанавливает, что киберзащита является частью основной задачи коллективной обороны Североатлантического союза, подтверждает, что международное право применяется в киберпространстве, стремится к дальнейшему развитию потенциала НАТО и союзников, а также интенсифицирует сотрудничество НАТО с промышленностью. Главным приоритетом является защита сетей, принадлежащих Альянсу и управляемых им.

Политика НАТО в области киберзащиты дополняется планом действий с конкретными целями и сроками осуществления по целому ряду тем, начиная с развития потенциала, образования, подготовки кадров и учений, а также партнерских отношений.

В 2018 году союзники договорились создать новый центр Киберпространственных операций в рамках усиленной командной структуры НАТО. Они также согласились с тем, что НАТО может использовать национальный кибернетический потенциал для своих миссий и операций.

Из вышесказанного можно сделать вывод о том, что в период, начиная с 2008 года и заканчивая современностью, НАТО сумело разработать систему специализированных механизмов и институтов оперативного и стратегического назначения для эффективной борьбы и противодействию кибертерроризму. Также в рамках НАТО были найдены инструменты в политической, дипломатической и военной сферах для борьбы с киберугрозами. Данным образом организация смогла повысить свою устойчивость в киберпространстве, а также разработала механизмы сдерживания, защиты и противодействия всему спектру киберугроз.

Поскольку киберугрозы бросают вызов государственным границам и организационным границам, НАТО взаимодействует с рядом стран-партнеров и другими международными организациями для укрепления международной безопасности.

Как отмечает Джефри Кэтон[30], в декларации Лиссабонского саммита 2010 года содержался призыв к НАТО более тесно сотрудничать с ЕС в области киберзащиты. Они разделяют общие интересы в программах обеспечения безопасности, осуществляемых обеими организациями, а также стремление не допускать ненужного дублирования ресурсного вклада. Что касается кибербезопасности, то ЕС и НАТО имеют схожие цели, но разные подходы.

Как для НАТО, так и для ЕС кибербезопасность является вопросом стратегического значения, оказывающим влияние на безопасность и оборону государств-членов и самих объединений. Обе организации ставят на первое место устойчивость и защиту своих собственных сетей и органов. При этом считая, что кибербезопасность отдельных государств-членов является сферой их национальной ответственности. Миссии этих двух организаций взаимодополняют друг друга: НАТО сосредоточивает свое внимание на аспектах безопасности и обороны кибербезопасности, а ЕС занимается более широким, главным образом невоенным кругом киберпространственных вопросов и аспектами внутренней безопасности.

Немаловажной считается работа ООН в сфере противодействия кибертерроризму. В рамках международной организации на повестке дня не раз поднимался вопрос о борьбе с данной проблемой.

Для примера можно рассмотреть Резолюцию Совета Безопасности ООН № 2178 от 24 сентября 2014 года[31]. В ней утверждается, что терроризм в его различных проявлениях представляет угрозу для всего мирового сообщества. Также в документе говорится о том, что террористы в последнее время стали все чаще прибегать к использованию компьютерных технологий для совершения атак. В связи с этим государства-члены ООН договорились о приложении совместных усилий в борьбе с данной

[30] Caton J. NATO cyberspace capability: a strategic and operational evolution [Электронный ресурс] - Strategic Studies Institute, US Army War College. – Режим доступа: www.jstor.org/stable/resrep11524. (дата обращения 22.04.2020).
[31] Резолюция Совета Безопасности ООН № 2178 [Электронный ресурс] : резолюция от 24.09.2014 - Режим доступа: https://undocs.org/ru/S/RES/2178(2014). (дата обращения: 22.04.2020).

проблемой, чтобы не позволить использование сетевых ресурсов и иных информационных технологий в террористической деятельности.

Кроме того следует упомянуть о Резолюции Генеральной Ассамблеи № 73/266 от 22 декабря 2018 года[32]. В резолюции сохраняется основная идея указанного выше документа. Однако подчеркивается необходимость наращивания координации и сотрудничества между государствами в борьбе с использованием высоких технологий преступными элементами, так как это может негативным образом отразится на целостности инфраструктуры государств, нарушая их безопасность. Также указывается, что данные меры должны гарантировать свободу технологического и информационного обмена с учетом уважения суверенитета государств.

Помимо этого использование информационно-коммуникационных технологий в террористических целях запрещено Резолюцией Генеральной Ассамблеи Интерпола № 10 от 22 сентября 2005 года[33]. В документе утверждается, что в организации обеспокоены эксплуатацией террористами интернет-технологий в качестве оружия для нападения. В связи с этим от стран-членов требуется беспрепятственное сотрудничество в рамках международных юрисдикций, основанное на уважении суверенитета наций. Также, странами-членами поощряется своевременное обеспечение передачи информации, которая может помочь в расследовании преступлений. Резолюция призывает государств-членов установить на законодательном уровне эффективные процедуры для расширения возможностей международных расследований и судебного преследования в отношении интернет ресурсов, поддерживающих террористов.

На основе сравнения вышеперечисленных международно-правовых инициатив, можно сделать вывод о том, что международные организации стали предпринимать все больше мер для более эффективного

[32] Резолюции Генеральной Ассамблеи № 73/266 [Электронный ресурс] : резолюция от 22.12.2018 - Режим доступа: https://undocs.org/ru/A/RES/73/266. (дата обращения: 22.04.2020).
[33] Interpol General Assembly Resolution № 10 of 22 September 2005 [Электронный ресурс]. - Режим доступа: https://www.interpol.int/content/download/6110/file/GA-2005-74-RES-10%20-%20Addressing%20Internet%20activities%20supporting%20terrorism.pdf. (дата обращения: 27.04.2020).

сотрудничества в сфере борьбы с кибертерроризмом. Это прежде всего связанно с повышением количества новых угроз исходящих из киберпространства. В ответ на данные вызовы государствам следует сосредоточиться на разработке систем по контролю над информационным потоком внутри сетевых ресурсов, при этом не выходя за правовые рамки международного и национального законодательства. Также, исходя из содержания международно-правовых инициатив, можно проследить общую идею того, что международные организации стремятся выработать общие международные стандарты в сфере борьбы с киберпреступностью. Данная "унификация" законодательства поможет в будущем избежать путаницы и двусмысленных трактовок. Помимо прочего, сотрудничество государств между собой в данной области может стать хорошим стимулом для дальнейшего изучения информационных систем и созданию ответных мер для пресечения кибератак.

Также важно рассмотреть деятельность государств в рамках БРИКС в которое входят Бразилия, Россия, Индия, Китай и ЮАР. БРИКС является объединением в рамках которого страны-участники направляют совместные усилия на закрепление политического влияния в своих регионах, а также на противодействие международным вызовам представляющим общую угрозу, в число которых входит проблема безопасности в информационном пространстве.

По мнению Е. С. Пелевиной[34] сотрудничество в сфере поддержания международной безопасности в информационном пространстве имеет большие перспективы в рамках объединения. Страны-члены выражают свое беспокойство по поводу возможности использования современных информационных технологий с целью ведения военно-политической борьбы и совершения актов кибертерроризма в киберпространстве.

[34] Пелевина, Е. С. Проблемы информационной безопасности стран БРИКС в контексте современных международных угроз / Е. С. Пелевина. [Электронный ресурс] // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Общество. Коммуникация. Образование. - 2016. - № 2. – С. 45-51. – Режим доступа: https://cyberleninka.ru/article/n/problemy-informatsionnoy-bezopasnosti-stran-briks-v-kontekste-sovremennyh-mezhdunarodnyh-ugroz. (дата обращения: 15.04.2020).

В 2015 г. прошел VII Международный IT-форум с участием стран БРИКС и ШОС[35]. По итогам форума страны БРИКС отметили следующие направления в рамках которых будет осуществляться их совместная деятельность по борьбе с кибертерроризмом:

- Атаки в информационной среде и кибертерроризм. В данном направлении отмечается необходимость обеспечения регулярного наблюдения за новейшими тенденциями технологического развития компьютерных систем по обнаружению и противодействию кибератакам на сетевые ресурсы. Также упоминается о наращивании интенсивности исследований в разработке методов борьбы с данным явлением.

- Безопасность средств связи. Целесообразным считается использование новых методов борьбы с киберпреступностью, которые позволят повысить общий уровень безопасности систем связи и информационных коммуникаций.

- Обеспечение информационной безопасности. Отмечается необходимость использования информационно-аналитических и экспертно-аналитических систем для управления критически важными объектами инфраструктуры, что способствует улучшению общего состояния обеспечения безопасности в киберпространстве. Также выдвигается Концепция «умного региона».

Также стоит упомянуть о важности практических мер предпринятых БРИКС для обеспечения безопасности в компьютерной среде. К примеру, в рамках объединения были разработаны новейшие системы в сфере борьбы с киберугрозами. Российская компания InfoWatch создала систему «щит», которая обеспечивает защищенную работу от информационных атак автоматизированных систем управления технологическими процессами, обеспечивающих функционирование промышленных предприятий. Уникальность данной системы заключается в том, что она способна

[35] Югорская Декларация Седьмого Международного IT-Форума с участием стран БРИКС и ШОС [Электронный ресурс] : декларация от 7.07.2015. // Режим доступа: https://itforum.admhmao.ru/2015/ugradeclaration. (дата обращения: 26.04.2020).

минимизировать сбои в работе систем управления и непредвиденные ситуации вызванных извне.

Кроме того стоит сделать акцент на сотрудничестве вне рамок БРИКС между Китаем и Россией. Нарастание международной угрозы кибертерроризма стало одной из предпосылок изменения законодательств РФ и КНР в сфере противодействия терроризму в киберпространстве. К примеру, Антитеррористический закон КНР[36] от 2015 года, содержит различные меры по борьбе с терроризмом, в информационном пространстве в том числе. Согласно документу компании предоставляющие услуги связи обязаны предоставлять органам государственной безопасности техподдержку с целью противодействия и предупреждения деятельности террористов в интернет среде. Также данные компании обязаны принимать участие в создании определенных мер направленных на защиту интернет пространства, в том числе отслеживать материалы публикуемые кибертеррористами. Таким образом, для недопущения распространения террористических материалов пропагандистской направленности правительство Китая проводит в стране политику ограничения свободы слова в информационном пространстве.

По мнению И. Чжэн[37], законодательство КНР и РФ имеет большие перспективы для развития как двустороннего, так и международного сотрудничества в сфере борьбы с кибертерроризмом.

В качестве примера автор приводит Двустороннее межправительственное Соглашение о сотрудничестве в области обеспечения международной информационной безопасности[38]. Данный документ укрепил российско-китайские отношения в сфере противодействия кибертерроризму. В соглашении отражена значимость и схожесть методов взаимодействия в

[36] Антитеррористический закон КНР [Электронный ресурс] : Закон КНР от 28.12.2015. - Режим доступа: http://news.mod.gov.cn/headlines/2015-12/28/content_4634331.htm. (дата обращения: 25.04.2020).
[37] Чжэн, И. Сотрудничество РФ и КНР в борьбе с кибертерроризмом / И. Чжэн. [Электронный ресурс] // Вестник МГОУ. - 2018. - № 2. – С. 204-212. – Режим доступа: https://cyberleninka.ru/article/n/sotrudnichestvo-rf-i-knr-v-borbe-s-kiberterrorizmom. (дата обращения 23.04.2020).
[38] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 2016 года // Режим доступа: http://docs.cntd.ru/document/420283259. (дата обращения: 26.04.2020).

сфере международной информационной России и Китая. Более того оно имеет практическое значение и прежде всего направлено на консолидацию совместных усилий для достижения общих целей, касающихся поддержания национальной и международной безопасности в киберпространстве. Также в документе отмечается необходимость создания правовых рамок для взаимодействия властей России и Китая, охватывающего всю сферу проблем относящихся к информационной безопасности.

Помимо этого в соглашении отмечается необходимость предпринять общие действия для более быстрого реагирования на вызовы представляющие особую угрозу в информационном пространстве. К ним относится противодействие применению компьютерных технологий для нарушения общепризнанных принципов и норм международного права, включая вмешательство во внутренние дела государств с целью нарушить суверенитет, дестабилизировать политическую и экономическую сферы общества. Также поднимается вопрос о взаимном обмене информацией и сотрудничестве в сфере разработки международно-правовых инициатив по противодействию киберпреступности.

Обобщая вышесказанное, можно сделать вывод, что на данный момент действия и инициативы государств в рамках БРИКС носят системный характер и охватывают большой спектр угроз исходящих из информационного пространства. Также стоит отметить новейшие разработки, которые проводятся в сфере сотрудничества в данной области. Таким образом, при помощи совместных усилий прилагаемых странами БРИКС противодействие кибертерроризму выходит на новый уровень, что напрямую отвечает интересам государств и обеспечивает создание более надежной системы защиты в киберпространстве. Помимо этого важно упомянуть о сотрудничестве России и Китая вне рамок данного политического объединения. Результатом взаимодействия государств в области противодействия кибертерроризму является значительно

проработанная нормативно-правовая база, которая затрагивает широкий круг вопросов, а также накопленный опыт в противодействии данной проблеме.

Помимо взаимодействия стран в рамках международных организаций и государственных объединений, они порой прибегают к сотрудничеству с корпорациями в сфере IT-технологий. Однако, в данном направлении развития совместных усилий, тоже имеются свои препятствия и барьеры.

На фоне роста проблемы распространения кибертерроризма у правительств и корпораций многих государств возникают трудности с созданием адекватных мер по реагированию на данный вид угроз.

По словам исследователя Ариэль Левитт[39]: “Объем и интенсивность активности пользователей в киберпространстве привлекли значительное внимание правительств. В настоящее время предпринимаются многочисленные и разнообразные усилия правительств и корпораций, направленные на борьбу с данной проблемой”.

Некоторые из них пытались выследить и преследовать киберпреступников. Другие создавали структуры для предотвращения и реагирования на особо вопиющий вид атак, а третьи пропагандировали более эффективные методы обеспечения кибербезопасности. Наиболее продвинутые игроки в корпоративном мире создали или расширили свои собственные операции по разведке киберугроз и методов кибербезопасности, применяемых к их собственным сетям, продуктам, услугам, и более того распространили их на всю цепочку своих поставок и клиентов. Данные усилия частных и государственных акторов продемонстрировали реальные перспективы для ограничения и пресечения киберугроз.

Например, многие крупные компании в сфере информационно-коммуникационных технологий разрабатывают более сложные стандарты и методы для повышения безопасности и надежности, а также

[39] Levite A. E. Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance [Электронный ресурс] - Report. Carnegie Endowment for International Peace. – Режим доступа: www.jstor.org/stable/resrep20984.5. (дата обращения 23.04.2020).

производительности киберпродуктов. Важность и выгоды от этих усилий не следует сбрасывать со счетов.

Также, автор поднимает проблему того, что зачастую корпорации сопротивляются навязчивому государственному регулированию и другим формам вмешательства в их внутренние дела, включая их практику управления киберрисками. Некоторые из этих препятствий вызваны традиционными проблемами частного сектора по отношению к государственному регулированию: издержки и бремя реализации, подверженность ответственности, связанной с соблюдением требований, а также рисками, связанными с сообщением о методах осуществления кибербезопасности правительству и общественности. Еще один источник сдерживания связан с нежеланием корпораций удовлетворять конкурирующие требования различных правительств, на территории которых они действуют, или даже с конкурирующими нормативными требованиями, предъявляемыми одним и тем же правительством.

Кроме того, стоит упомянуть о помехах, вызванных коммерческой конкуренцией и правительственным регулированием. Регулирование трансграничных потоков данных и антимонопольные меры представляют собой особую проблему для частного сектора по борьбе с киберпреступностью, особенно в контексте неравномерной международной нормативно-правовой среды. К этим опасениям прибавляются соображения из политической и национальной безопасности, а также коммерческая конкуренция. Кроме того, возникает беспокойство по поводу потенциальных рисков, создаваемых обменом конфиденциальной информации о методах обеспечения безопасности. Эти факторы не только являются барьером, но зачастую напрямую препятствуют объединению совместных усилий государств и корпораций по обмену передовым опытом.

Однако, бывают случаи когда сами корпорации являются инициаторами сотрудничества с государствами. Так, по словам, вице-президента и заместителя начальника юридического управления корпорации

Microsoft, Стива Крауна[40]: “*Microsoft* настоятельно призывает к государственному регулированию информационного пространства. Компания действительно одобряет разумное регулирование со стороны правительства. В компании считают, что если на практике удастся оказать помощь в установлении правил, которые обеспечат позитивное развитие, минимизируют риски нарушения прав пользователей сети и облегчат достижение целей, то для компании это наилучший вариант действий. Вот почему в Microsoft уверены в многостороннем взаимодействии, поскольку в нем можно увидеть путь к установлению мирной, открытой, доступной и безопасной онлайн-среды, отвечающей интересам большинства стран”.

Основываясь на вышесказанном, можно прийти в выводу, что на сегодняшний день основные инновации и инициативы по борьбе с кибертерроризмом исходят от негосударственных акторов. Безопасность в данной сфере сосредоточена в их руках, что не совсем приемлемо для правительств многих государств. Отсюда вытекают различные проблемы при их взаимодействии. Рычаги давления органов власти могут привести к “вынужденному” сотрудничеству между правительствами и корпорациями в сфере IT- технологий, что неблагоприятным образом сказывается на эффективности данного взаимодействия. С другой стороны, бывают примеры когда государства и корпорации видят положительные перспективы в усилении контроля над информационным пространством для гармонизация и создания мирной обстановки в сети интернет и минимизации ее использования в корыстных целях.

## 2.2 Нормативно-правовое регулирование сферы борьбы с кибертерроризмом

На сегодняшний день проблема кибертерроризма представляет угрозу не для конкретных государств, а для всего международного сообщества. Борьба с преступлениями в киберпространстве входит в число одних из

[40] Microsoft призывает к государственному регулированию киберпространства [Электронный ресурс]. - Режим доступа: https://russiancouncil.ru/analytics-and-comments/interview/microsoft-prizyvaet-k-gosudarstvennomu-regulirovaniyu-kiberprostranstva. (дата обращения 24.04.2020).

основных задач государств по поддержанию внутренней и внешней безопасности. Стоит отметить, что в некоторых государствах существуют хорошо проработанные международно-правовые инициативы для противодействия кибертерроризму. Тем не менее, преступники в информационном пространстве с каждым днем наращивают свой ресурсный потенциал, тем самым модернизируя методы совершения противоправных действий в интернете. Вследствие этого государствам необходимо постоянно обновлять и совершенствовать антитеррористическое законодательство на национальном и международном уровнях.

В качестве примера можно привести деятельность Европейского союза и Российской Федерации по разработке международно-правовых инициатив для противодействия кибертерроризму.

В рамках ЕС существует немалое количество нормативно-правовых актов регулирующих информационную сферу. По мнению Н. О. Мороз[41]: “Правовой основой регулирования сотрудничества государств-членов ЕС в борьбе с киберпреступностью является первичное (учредительные договоры) и вторичное право ЕС (регламенты, директивы, решения)”.

Первые положения регулирующие сферу противодействия преступности в киберпространстве, были включены в международную Конвенцию о киберпреступности от 23 ноября 2001 года[42], которая является важным документом в области противодействия данному виду преступлений. Конвенция была подписана тридцатью странами Европы и Америки. В документе выделяются основные виды преступлений в информационной среде, а именно: противозаконный доступ в киберпространство и перехват информации в нем, воздействие на данные и компьютерные системы.

[41] Мороз, Н. О. Особенности международно-правового сотрудничества в борьбе с киберпреступностью в рамках ЕС / Н. О. Мороз // Вестник Марийского государственного университета. Серия “Исторические науки. Юридические науки”. - 2018. - № 4. – С. 88.

[42] Конвенция Совета Европы о киберпреступности [Электронный ресурс] : конвенция от 23.11.2001. // Справочная правовая система «ГАРАНТ». - Режим доступа: https://base.garant.ru/4089723/. (дата обращения: 23.04.2020).

В течение 2001-2005 годов Российская Федерация принимала активное участие в создании проекта Конвенции Совета Европы о предупреждении терроризма от 16 мая 2005 года[43] и ратифицировала его в числе первых государств. В документе отмечается, что для повышения эффективности противодействия терроризму необходимо модернизировать национальное законодательство, а также предпринять меры для обеспечения международного расследования данного рода преступлений и поддержки международного сотрудничества. Данная Конвенция в какой-то мере ограничивала деятельность кибертеррористов, но не оказывала на них большого влияния, так как на территории других государств они могли безнаказанно осуществлять свою деятельность.

Кроме того, в качестве инструмента регулирования законодательства в информационной среде выступали рамочные решения, принимаемые Советом ЕС. Примером может послужить Рамочное решение Совета 2005/222 об атаках на информационные системы.

Следующим основополагающим документом в сфере борьбы с кибертерроризмом принятым Советом ЕС была Директива Европейского Парламента и Совета об атаках на информационные системы от 12 августа 2013 года[44], которая заменила предшествующее ей Рамочное соглашение 2005/222.

Директива об атаках на информационные системы от 12 августа 2013 г. вводила под запрет незаконное подключение к компьютерной системе, а также создание помех в ее работе. Запрещался несанкционированный доступ к личным данным и их перехват, использование компьютерных систем и программного обеспечения для совершения противозаконных действий. Цель данного документа заключалась в том, чтобы приблизить уголовное законодательство государств-членов в области атак на информационные

[43] Конвенции Совета Европы о предупреждении терроризма [Электронный ресурс] : конвенция от 16.05.2005. - Режим доступа: http://docs.cntd.ru/document/901937508. (дата обращения: 23.04.2020).
[44] Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems of 12 August 2013 [Электронный ресурс]. - Режим доступа: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF. (дата обращения: 20.04.2020).

системы путем установления минимальных правил определения уголовных преступлений и соответствующих санкций и улучшить сотрудничество между компетентными органами, включая полицию и другие специализированные правоохранительные службы государств-членов.

Одним из важнейших документов в области информационной обороны ЕС была Стратегия кибербезопасности от 7 февраля 2013 года[45]. Согласно ей ЕС должен защищать информационную среду, обеспечивающую максимально возможную свободу и безопасность на благо каждого человека. При этом признавалось, что основная задача государств-членов заключается в решении проблем безопасности в киберпространстве. Данная стратегия предлагает конкретные действия, которые могут повысить общую эффективность ЕС.

Данная стратегия сформулировала перед ЕС пять стратегических приоритетов:

- достижение киберустойчивости;

- радикальное сокращение киберпреступности;

- разработка политики и возможностей киберзащиты, связанных с общей политикой безопасности и обороны;

- разработка промышленных и технологических ресурсов для обеспечения кибербезопасности;

- выработка согласованной международной политики в области киберпространства для Европейского Союза и продвижения его основных ценностей.

Как отмечает Джобел Векино[46], в последнее время национальные правоохранительные органы европейских государств начали участвовать во вновь созданных международных институтах, ориентированных на

[45] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace of 7 February 2013 [Электронный ресурс]. - Режим доступа: https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN. (дата обращения: 20.04.2020).

[46] Vecino J. United by Necessity: Conditions for Institutional Cooperation against Cybercrime [Электронный ресурс] - The Cyber Defense Review. – Режим доступа: www.jstor.org/stable/26846124. (дата обращения 21.04.2020).

смягчение последствий киберпреступности. Одним из примеров этого является Европол.

Использование Европола в качестве платформы для сотрудничества предполагает принятие заранее определенных политических процедур и целей, которые могут не совпадать с выбранными государствами-членами политическими целями. Однако государства имеют возможность влиять на эти политические цели, если они решат внести свой вклад в их формирование и принятие. Это делает Европол полезным примером для анализа условий, которые приводят к сотрудничеству в борьбе с киберпреступностью без какой-либо формы иерархического принуждения.

Д. Векино сопоставляет взаимодействие между государствами и организациями в контексте киберпреступности с конкретными классификациями. Он предлагает пять категорий сотрудничества в борьбе с киберпреступностью:

- наращивание потенциала;
- обмен информацией;
- нормативно-правовая деятельность;
- проведение уголовных расследований и сбор разведывательных данных;
- лоббирование.

В рамках работы Европола в 2019 году был опубликован документ “Оценка угрозы организованной преступности в интернете (IOCTA)[47]”.

Согласно ему, ограничение способности террористов осуществлять трансграничные нападения путем нарушения их потока пропаганды и приписывания им преступлений, связанных с терроризмом в интернете, требует постоянного и более активного сотрудничества в борьбе с терроризмом и обмена информацией между правоохранительными органами, а также с частным сектором.

[47]Internet Organised Crime Threat Assessment (IOCTA) of 2019 [Электронный ресурс]. - Режим доступа: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019. (дата обращения: 27.04.2020).

Подчеркивается, что кроссплатформенное сотрудничество и многосторонний протокол реагирования на кризисные ситуации в отношении террористического контента в интернете будут иметь важное значение для управления кризисными ситуациями после террористического нападения. Более глубокое понимание работы новых и возникающих технологий является приоритетом в разработке эффективной стратегии предотвращения дальнейших правонарушений.

Из всего вышеизложенного можно сделать вывод, что ЕС прибегает к системному методу для регулирования совместной деятельности государств-членов ЕС в борьбе с преступлениями в информационной среде, который имеет правовую и институциональную составляющие. Также стоит отметить, что содержания нормативно-правовых актов, регулирующих сотрудничество государств-членов ЕС в борьбе с киберпреступностью отражает направление ЕС на унификацию и стандартизацию законодательства в области кибербезопасности, также ставятся цели о наращивании информационно-ресурсного потенциала для успешного претворения данной политики в жизнь. Кроме того можно отметить поощрение международного сотрудничества для сдерживания данного вида угрозы.

С конца 1990-х годов, во внешней политике Российской Федерации активизируется направление по борьбе с кибертерроризмом. Россия начинает содействовать в выработке международно-правовых норм, регулирующих сферу противодействия преступлениям в информационном пространстве.

Тем не менее, как отмечает В. А. Прокопьева[48] предпринимаемые действия имели формальный характер, и на практике, зачастую, показывали свою неэффективность. Тому подтверждением является ежегодная статистика кибертеррористических актов против крупных компаний и государственных структур число которых возрастает в большинстве стран мира, в том числе и в России.

[48] Прокопьева, В. А. Политика противодействия кибертерроризму в современной России / В. А. Прокопьева // Вестник социально-гуманитарного образования и науки. - 2016. - № 4. – С. 33.

Стоит отметить, что Российская Федерация заключила множество двусторонних договоров о правовой помощи по уголовным делам с другими странами. Они являются полезным инструментом во взаимодействии государств относительно сферы противодействия преступности, однако, с другой стороны, опыт показывает, что для борьбы с кибертерроризмом этого недостаточно и от стран требуется создание более гибкая структура в данной области. Прежде всего это связанно с тем, что направление и исполнение запросов о правовой помощи в рамках двусторонних договоров занимает достаточно большое время.

В России за последние десятилетия был выработан ряд нормативно-правовых актов, которые определяют подходы по обеспечению информационной безопасности внутри страны. К примеру, можно выделить Федеральный Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 2006 года[49]. Данный закон регулирует отношения в сфере передачи, производства и распространения информации, а также применения информационных технологий. Согласно ему запрещается заниматься распространением материалов доступ к которым ограничен на территории страны.

Также стоит уделить внимание Основам государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г[50]. Согласно ст. 9 целью государственной политики в сфере информационной безопасности является участие в создании международного правового режима, способствующему выработке ряда условий для формирования системы международной безопасности в информационном пространстве на многостороннем уровне. В ст. 10

[49] Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон РФ от 27.07.2006 № 149-ФЗ ред. от 03.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=349433&fld=134&dst=100008,0&rnd=0.46940131337595936#02575296435678198. (дата обращения: 25.04.2020).

[50] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года от 24.07.2013 // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_178634. (дата обращения: 24.04.2020).

обозначены задачи направленные на реализацию государственной политики в информационном пространстве, среди них: разработка мер способных снизить уровень угрозы применения компьютерных технологий в преступных целях, создание инструментов международного сотрудничества и повышение его эффективности в целом и др. Кроме того, в качестве приоритетного направлениями государственной политики РФ отмечается значимость международных контактов и консультаций в рамках международных объединений ШОС и БРИКС.

Немаловажный вклад в развитии системы противодействия кибертерроризму вносит Доктрина информационной безопасности Российской Федерации от 2016 года[51]. В документе подчеркивается необходимость укрепления равноправного стратегического сотрудничества в сфере безопасности в киберпространстве. Также выражаются опасения по поводу увеличения угроз в киберпространстве, связанных с расширением сфер использования современных технологий. В связи с этим отмечается, что при введении в эксплуатацию новых компьютерных технологий в какие-либо структуры без увязки с обеспечением информационной безопасности неблагоприятным образом сказывается на общем состоянии безопасности в киберсреде.

Кроме того, в 2017 году был издан Указ Президента РФ “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы”[52]. Приоритетными целями данного Указа являются: развитие человеческого потенциала, обеспечение информационной безопасности граждан и государства и др. Подчеркивается необходимость постоянного мониторинга и анализа угроз исходящих из информационного пространства. Также поднимается вопрос о создании единых сетей электросвязи

[51] Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс] : Указ Президента РФ от 5.12.2016 № 646 // Справочная правовая система «ГАРАНТ». - Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456224. (дата обращения: 25.04.2020).
[52] О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы [Электронный ресурс] : Указ Президента РФ от 9.05.2017 № 203 // Справочная правовая система «ГАРАНТ». - Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71570570. (дата обращения: 24.04.2020).

государственных органов для обеспечения безопасности в киберпространстве.

В Федеральном Законе «О безопасности критической информационной инфраструктуры Российской Федерации» от 2017 года[53] говорится о государственной системе по обнаружению информационных угроз. Согласно документу данная система является единым территориально распределенным комплексом, усилия и ресурсы которого направлены на обнаружение и противодействие атакам в киберпространстве посредством сбора, накопления и анализа информации.

Проанализировав нормативно-правовые акты РФ в сфере противодействия информационным угрозам можно заключить, что основные усилия государства направлены на создание четко отлаженной системы по борьбе с киберпреступностью. Неоднократно в документах поднимается вопрос о консолидации усилий по совместному противодействию преступлениям в информационном пространстве на международном уровне, необходимости разработки международно-правовых инициатив, так как в последние годы данный вид правонарушений приобрел всеобъемлющий характер. Отмечается важность межгосударственных контактов в рамках политических и региональных объединений на примере БРИКС и ШОС. Внутри государства постоянно совершенствуются инструменты для противодействия киберпреступности. Однако, стоит отметить тот факт, что в России отсутствуют определенные государственные структуры, которые могли бы вести борьбу с киберпреступлениями и заниматься разработкой технических средств для данных целей. Государству требуется обеспечить условия для сотрудничества с правоохранительными органами различных стран, обновить законодательную базу, которая позволит вести преследование за преступниками в сети интернет. Также сотрудничество с

[53] О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс] : федер. закон РФ от 26.07.2017 № 187-ФЗ // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220885&fld=134&dst=1000000001,0&rnd=0.42290954991783236#007164448036500382. (дата обращения: 23.04.2020).

частным сектором и современными IT-компаниями могло бы повысить эффективность принимаемых мер направленных на противодействие кибертерроризму.

# ЗАКЛЮЧЕНИЕ

Подводя итог можно заключить, что на сегодняшний день существует немалое количество международно-правовых инициатив, международных площадок, форумов для противодействия кибертерроризму. Данные инструменты затрагивают большой спектр угроз исходящих из информационного пространства и, в какой-то мере, являются ограничительным фактором для распространения киберпреступности. Однако, как показывает практика, предпринимаемые действия не дают достичь должного результата. Это является следствием того, что инициативы предпринимаемые государствами по большей части ориентированы на укрепление внутреннего законодательства для борьбы с преступлениями в информационном пространстве. Тем не менее, стоит помнить, что кибертерроризм является проблемой не отдельно взятого государства, а всего мирового сообщества в целом и требует международного решения. Государства должны объединить общие усилия для унификации законодательства в сфере противодействия киберпреступности посредством международных соглашений или в рамках работы межправительственных, региональных объединений. Кроме того, государствам стоит обратить внимание на разработки и меры по противодействию данной проблеме предпринимаемыми крупнейшими IT-компаниями, так как на сегодняшний день основные инновации и инициативы по борьбе с кибертерроризмом исходят от негосударственных акторов. Безопасность в данной сфере сосредоточена в их руках.

Кибертерроризм является результатом глобализационных процессов в экономической, политической и культурной сферах происходящих во всем мире. Развитие современных информационных технологий является предпосылкой распространения кибертерроризма. Вследствие этого киберпространство становится все более привлекательным для террористов.

Помешать данным последствиям научного-технического прогресса, на данный момент, не представляется возможным.

Преступления в киберпространстве несут в себе большую угрозу для общества. Органы правопорядка большинства государств, пока что не могут противостоять кибертерроризму в должной мере ввиду отсутствия хорошо проработанной нормативно-правовой базы. Также стоит отметить тот факт, что какая-то часть информации о методах борьбы с киберпреступностью и статистика преступлений не подлежит общественной огласке.

Подводя итог, можно заключить, что в международном сообществе на данный момент пока отсутствуют эффективные международно-правовые инициативы по противодействию кибертерроризму, что ставит перед ним задачу не только выработать единые международно-правовые стандарты, но и обеспечить их осуществление каждым государством.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

## I. Нормативные

1. Антитеррористический закон КНР [Электронный ресурс] : Закон КНР от 28.12.2015. - Режим доступа: http://news.mod.gov.cn/headlines/2015-12/28/content_4634331.htm. (дата обращения: 25.04.2020).

2. Концепция противодействия терроризму в Российской Федерации [Электронный ресурс] : концепция от 05.10.2009. // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_92779. (дата обращения: 25.04.2020).

3. Конвенция Совета Европы о киберпреступности [Электронный ресурс] : конвенция от 23.11.2001. // Справочная правовая система «ГАРАНТ». - Режим доступа: https://base.garant.ru/4089723/. (дата обращения: 23.04.2020).

4. Конвенции Совета Европы о предупреждении терроризма [Электронный ресурс] : конвенция от 16.05.2005. - Режим доступа: http://docs.cntd.ru/document/901937508. (дата обращения: 23.04.2020).

5. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [Электронный ресурс] : Указ Президента РФ от 15.01.2013 № 31с ред. от 22.12.2017. // Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=286045&fld=134&dst=1000000001,0&rnd=0.6720959085752711#01785599082758227. (дата обращения: 25.04.2020).

6. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон РФ от 27.07.2006 № 149-ФЗ ред. от 03.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа:

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=349433&fld=134&dst=100008,0&rnd=0.46940131337595936#02575296435678198. (дата обращения: 25.04.2020).

7. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс] : Указ Президента РФ от 5.12.2016 № 646 // Справочная правовая система «ГАРАНТ». - Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456224. (дата обращения: 25.04.2020).

8. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года от 24.07.2013 // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_178634. (дата обращения: 24.04.2020).

9. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы [Электронный ресурс] : Указ Президента РФ от 9.05.2017 № 203 // Справочная правовая система «ГАРАНТ». - Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71570570. (дата обращения: 24.04.2020).

10. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс] : федер. закон РФ от 26.07.2017 № 187-ФЗ // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220885&fld=134&dst=1000000001,0&rnd=0.42290954991783236#007164448036500382. (дата обращения: 23.04.2020).

11. Резолюция Совета Безопасности ООН № 2178 [Электронный ресурс] : резолюция от 24.09.2014 - Режим доступа: https://undocs.org/ru/S/RES/2178(2014). (дата обращения: 22.04.2020).

12. Резолюции Генеральной Ассамблеи № 73/266 [Электронный ресурс] : резолюция от 22.12.2018 - Режим доступа: https://undocs.org/ru/A/RES/73/266. (дата обращения: 22.04.2020).

13. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента РФ от 31 декабря 2015 г. № 683 [электронный ресурс] // Справочная правовая система «ГАРАНТ». - Режим доступа: http://www.garant.ru/hotlaw/federal/688504/. (дата обращения: 25.04.2020).

14. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 2016 года // Режим доступа: http://docs.cntd.ru/document/420283259. (дата обращения: 26.04.2020).

15. Югорская Декларация Седьмого Международного IT-Форума с участием стран БРИКС и ШОС [Электронный ресурс] : декларация от 7.07.2015. // Режим доступа: https://itforum.admhmao.ru/2015/ugradeclaration. (дата обращения: 26.04.2020).

16. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace of 7 February 2013 [Электронный ресурс]. - Режим доступа: https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN. (дата обращения: 20.04.2020).

17. Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems of 12 August 2013 [Электронный ресурс]. - Режим доступа: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF. (дата обращения: 20.04.2020).

18. Internet Organised Crime Threat Assessment (IOCTA) of 2019 [Электронный ресурс]. - Режим доступа: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019. (дата обращения: 27.04.2020).

19. Interpol General Assembly Resolution № 10 of 22 September 2005 [Электронный ресурс]. - Режим доступа: https://www.interpol.int/content/download/6110/file/GA-2005-74-RES-10%20-%20Addressing%20Internet%20activities%20supporting%20terrorism.pdf. (дата обращения: 27.04.2020).

20. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation. Active Engagement, Modern Defence of 2010 [Электронный ресурс]. - Режим доступа: https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf. (дата обращения: 17.04.2020).

21. Uniting and Strengthening Americaby Providing Appropriate Tools Requiredto Interceptand Obstruct Terrorism Act of 2001 [Электронный ресурс]. - Режим доступа: https://grants.nih.gov/grants/policy/select_agent/Patriot_Act_2001.pdf. (дата обращения: 09.04.2020).

## II. Специальные

22. Асеев, С. Ю. Проблема определения кибертерроризма / С. Ю. Асеев, В. А. Воронцов. [Электронный ресурс] // Общество и цивилизация. - 2016. - № 2. - С. 49-53. – Режим доступа: https://www.elibrary.ru/item.asp?id=26399093. (дата обращения: 10.04.2020).

23. Бураева, Л. А. Кибертерроризм в молодежной среде / Л. А. Бураева. [Электронный ресурс] // Проблемы экономики и юридической практики. - 2016. - № 2. – С. 271–274. – Режим доступа: https://www.elibrary.ru/item.asp?id=25903441. (дата обращения: 18.04.2020).

24. Бураева, Л. А. Мировой опыт противодействия экстремизму и терроризму в глобальном информационном пространстве / Л. А. Бураева. [Электронный ресурс] // Теория и практика общественного развития. - 2015. - № 18. - С. 131-134. – Режим доступа: https://cyberleninka.ru/article/n/mirovoy-opyt-protivodeystviya-ekstremizmu-i-terrorizmu-v-globalnom-informatsionnom-prostranstve. (дата обращения: 18.04.2020).

25. Вехов, В. Б. Проблемы борьбы с кибертерроризмом / В. Б. Вехов, С. А. Ковалев. [Электронный ресурс] // Правопорядок: история, теория, практика. - 2018. - № 1. – С. 89-93. – Режим доступа: https://cyberleninka.ru/article/n/problemy-borby-s-kiberterrorizmom. (дата обращения: 08.04.2020).

26. Гаврилов, Ю. В. Современный терроризм: сущность, типология, проблемы противодействия / Ю. В. Гаврилов, Л. В. Смирнов. – Москва : ЮИ МВД РФ, 2003. - 66 с.

27. Галушкин, А. А. К вопросу о кибертерроризме и киберпреступности / А. А. Галушкин. [Электронный ресурс] // Вестник РУДН. Серия: Юридические науки. - 2014. - № 2. – С. 44-49. – Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-i-kiberprestupnosti. (дата обращения: 17.04.2020).

28. Диденко, А. И. Противодействие кибертерроризму / А. И. Диденко. [Электронный ресурс] // Отечественная юриспруденция. - 2016. - № 11. – С. 21-26. – Режим доступа: https://cyberleninka.ru/article/n/protivodeystvie-kiberterrorizmu. (дата обращения: 05.04.2020).

29. Кошечкина, Е. А. К вопросу о проблемах противодействия кибертерроризму / Е. А. Кошечкина. // ОНВ. ОИС. - 2017. - № 4. – С. 97-101.

30. Карамова, Э. И. К вопросу о кибертерроризме в глобализирующемся мире / Э. И. Карамова, С. М. Фомин. [Электронный ресурс] // Социально-политические науки. - 2016. - № 3. – С. 154-155. – Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-v-globaliziruyuschemsya-mire. (дата обращения: 20.04.2020).

31. Казаковцев, А. В. НАТО и кибербезопасность / А. В. Казаковцев. [Электронный ресурс] // Вестник ВолГУ. История. Регионоведение. Международные отношения. - 2012. - № 2. – С. 109-113. – Режим доступа: https://cyberleninka.ru/article/n/nato-i-kiberbezopasnost. (дата обращения: 24.04.2020).

32. Мазуров, В. А. Кибертерроризм: понятие, проблемы противодействия / В. А. Мазуров. [Электронный ресурс] // Доклады ТУСУР. - 2010. - № 1-1. – С. 41-45. – Режим доступа: https://cyberleninka.ru/article/n/kiberterrorizm-ponyatie-problemy-protivodeystviya. (дата обращения: 04.04.2020).

33. Мороз, Н. О. Особенности международно-правового сотрудничества в борьбе с киберпреступностью в рамках ЕС / Н. О. Мороз // Вестник Марийского государственного университета. Серия “Исторические науки. Юридические науки”. - 2018. - № 4. – С. 87-94.

34. Прокопьева, В. А. Политика противодействия кибертерроризму в современной России / В. А. Прокопьева // Вестник социально-гуманитарного образования и науки. - 2016. - № 4. – С. 31-38.

35. Пелевина, Е. С. Информационные угрозы кибертерроризма / Е. С. Пелевина. [Электронный ресурс] // Евразийский Союз Ученых. - 2015. - № 11-2. – С. 100-103. – Режим доступа: https://cyberleninka.ru/article/n/informatsionnye-ugrozy-kiberterrorizma. (дата обращения: 11.04.2020).

36. Пелевина, Е. С. Проблемы информационной безопасности стран БРИКС в контексте современных международных угроз / Е. С. Пелевина. [Электронный ресурс] // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Общество. Коммуникация. Образование. - 2016. - № 2. – С. 45-51. – Режим доступа: https://cyberleninka.ru/article/n/problemy-informatsionnoy-bezopasnosti-stran-briks-v-kontekste-sovremennyh-mezhdunarodnyh-ugroz. (дата обращения: 15.04.2020).

37. Пользователи интернета в мире [Электронный ресурс]. - Режим доступа: https://www.internetworldstats.com/stats.htm. (дата обращения 02.04.2020).

38. Чжэн, И. Сотрудничество РФ и КНР в борьбе с кибертерроризмом / И. Чжэн. [Электронный ресурс] // Вестник МГОУ. -

2018. - № 2. – С. 204-212. – Режим доступа: https://cyberleninka.ru/article/n/sotrudnichestvo-rf-i-knr-v-borbe-s-kiberterrorizmom. (дата обращения 23.04.2020).

39. Шогенов, Т. М. Терроризм в условиях глобализации. Кибертерроризм / Т. М. Шогенов. [Электронный ресурс] // Социально-политические науки. - 2018. - № 3. – С. 181-182. – Режим доступа: https://cyberleninka.ru/article/n/terrorizm-v-usloviyah-globalizatsii-kiberterrorizm. (дата обращения 03.04.2020).

40. Caton J. NATO cyberspace capability: a strategic and operational evolution [Электронный ресурс] - Strategic Studies Institute, US Army War College. – Режим доступа: www.jstor.org/stable/resrep11524. (дата обращения 22.04.2020).

41. Denning D. E. Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy [Электронный ресурс] - Georgetown University. – Режим доступа: http:// http://www.iwar.org.uk/cyberterror/resources/denning.htm. (дата обращения 03.04.2020).

42. Denning D. E. “Cyberterrorism”, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services [Электронный ресурс] - US House of Representatives. – Режим доступа: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. (дата обращения 08.04.2020).

43. International Institute for Counter-Terrorism (ICT). Cyber Report 24 September-November 2017 [Электронный ресурс]. – Режим доступа: www.jstor.org/stable/resrep17687.7. (дата обращения 09.04.2020).

44. Vecino J. United by Necessity: Conditions for Institutional Cooperation against Cybercrime [Электронный ресурс] - The Cyber Defense Review. – Режим доступа: www.jstor.org/stable/26846124. (дата обращения 16.04.2020).

45. Kenney M. Cyberterrorism in a post-stuxnet world [Электронный ресурс] - Strategic Studies Institute, US Army War College. – Режим доступа: www.jstor.org/stable/resrep11980.9. (дата обращения 09.04.2020).

46. Levite A. E. Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance [Электронный ресурс] - Report. Carnegie Endowment for International Peace. – Режим доступа: www.jstor.org/stable/resrep20984.5. (дата обращения 23.04.2020).

47. Microsoft призывает к государственному регулированию киберпространства [Электронный ресурс]. - Режим доступа: https://russiancouncil.ru/analytics-and-comments/interview/microsoft-prizyvaet-k-gosudarstvennomu-regulirovaniyu-kiberprostranstva. (дата обращения 24.04.2020).

48. Williams P. Introduction. Cyberspace: malevolent actors, criminal opportunities, and strategic competition [Электронный ресурс] - Strategic Studies Institute, US Army War College. – Режим доступа: www.jstor.org/stable/resrep11980.4. (дата обращения 08.04.2020).

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт

кафедра международного права

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т.Ю. Сидорова
подпись инициалы, фамилия
«01» 06 2020 г.

# БАКАЛАВРСКАЯ РАБОТА

41.03.05. Международные отношения
профиль подготовки 41.03.05.01 Международные отношения и внешняя политика

Международные инициативы в сфере борьбы с кибертерроризмом

Руководитель _____ 10.06.2020 доцент, к.филос.н М.С. Бухтояров
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ 10.06.2020 В.А. Погодаев
подпись, дата инициалы, фамилия

Красноярск 2020