Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
**«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

Юридический институт

кафедра международного права

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т.Ю. Сидорова
подпись инициалы, фамилия
«____» _____ 2022 г.

# БАКАЛАВРСКАЯ РАБОТА

41.03.05. Международные отношения

Информационные войны в медиа-пространстве

| | | | |
|---|---|---|---|
| Руководитель | _____ | доцент, к.ю.н | Э.А. Павельева |
| | подпись, дата | должность, ученая степень | инициалы, фамилия |
| Выпускник | _____ | | К.В. Рубан |
| | подпись, дата | | инициалы, фамилия |

Красноярск 2022

**СОДЕРЖАНИЕ**

# ВВЕДЕНИЕ

В последнее десятилетие общество засвидетельствовало феноменальный рост возможностей механизмов управления информацией, и значение этих возможностей для систем национальной безопасности государств сейчас начинает в полной мере осознаваться мировыми политическими лидерами.

Развитие технологий в современную эпоху способствовало возникновению так называемых «информационных войн», которые подразумевают использование информации в качестве оружия, направленного против определённого противника. Информационные войны ведутся с использованием ряда тактик, таких как, например, внедрение методов взлома программного обеспечения для распространения вредоносных программ в стратегически важные компьютерные системы для кражи конфиденциальных данных, либо с целью повреждения вражеской системы безопасности.

Нет сомнения в том, что концепция информационной войны имеет огромное политическое, техническое, оперативное и юридическое значение для вооружённых сил повсеместно, поскольку достижения в области компьютерных технологий обладают достаточным потенциалом для того, чтобы кардинально изменить состояние военного командования и управления любого государства. Из-за нематериального характера ущерба, причиняемого операциями в рамках информационной войны, международному праву становится сложно регулировать данные процессы, что позволяет государствам и негосударственным субъектам использовать информационную войну для получения тактического и стратегического преимущества.

Несмотря на результаты использования концепции информационной войны в военно-техническом аспекте, её ключевой составляющей остаётся психологический фактор. Медиапространство, в частности, СМИ и социальные сети, является наиболее эффективным инструментом для распространения пропаганды и дезинформации в современных информационных войнах со стороны как государственных, так и негосударственных субъектов. Всё больше

стран сейчас вступает в борьбу за влияние в социальных сетях, цифровой суверенитет и господство в информационном поле, где все, без преувеличения, заявления нацелены на людей в обществе, влияя на их убеждения и поведение, или даже снижение доверия к правительству.

Таким образом, вместо того, чтобы атаковать военную или экономическую инфраструктуру, государственные и негосударственные субъекты могут получать доступ к регулярным потокам онлайн-информации через социальные сети, чтобы влиять на сетевые группы в той или иной стране. Противники на политической арене теперь стремятся контролировать и использовать механизм трендов в социальных сетях, чтобы нанести ущерб интересам своего геополитического врага, дискредитировать государственные и частные институты и посеять внутренние раздоры, подрывая позиции оппонента изнутри, при этом не растрачивая собственные ресурсы на ведение открытого вооружённого противостояния со всеми сопутствующими рисками.

**Актуальность** работы обусловлена природой изучаемых явлений: международные отношения – это постоянно меняющаяся, динамичная среда, ввиду чего неизменно актуальная для анализа и изучения, особенно в последние годы, когда мировое научное сообщество ведёт речь о формировании нового миропорядка; информационное пространство же находится вне физических границ и всё больше играет роль в жизни каждого гражданина, все люди зависимы от контента, который они потребляют посредством масс-медиа. Социальная природа человека привела к тому, что традиционные модели СМИ уступили место более удобной форме общения и потребления информации, а злоумышленники быстро нашли способы, как использовать открытость Интернета и социальных сетей в качестве инструмента для распространения пропаганды и «фейковых новостей». СМИ, в свою очередь, ввиду того, что несут за собой функцию фильтрации, отбора и распространения значимой информации, а следовательно, являются мощным средством политического манипулирования и воздействия на сознание масс, стали связующим звеном для ведения информационных войн и кибероперaций.

**Целью** данной выпускной квалификационной работы является раскрытие сущности информационной войны, а также анализ влияния, оказываемого ею на мировые политические процессы, в частности, при помощи средств массовой информации.

Для реализации указанных целей были поставлены следующие **задачи**:

- определить понятие и особенности информационной войны,

- изучить виды и методы информационной войны,

- разграничить понятия «информационная война», «психологическая война», «кибервойна», «пропаганда»,

- проанализировать существующие нормы международного права в сфере информационного противоборства,

- проанализировать, какими способами средства массовой информации влияли на общественные и политические процессы в ходе некоторых военно-политических конфликтов.

**Объектом исследования** работы является комплекс стратегий, направленных на нанесение ущерба информационной инфраструктуре или репутации противника, путём распространения специально отобранных информационных материалов, а также противодействия подобным действиям в свою сторону, с целью реализации политических, военных и иных задач.

**Предметом исследования** работы являются информационные войны, реализующиеся посредством средств массовой коммуникации.

Исследование было основано на отечественных и зарубежных новостных источниках, научных работах таких исследователей как Барабаш Виктор Владимирович и Котеленец Елена Анатольевна – профессоров Российского университета дружбы народов, и некоторых других отечественных и зарубежных специалистов.

**Структура работы** обусловлена целями и задачами исследования. Выпускная квалификационная работа состоит из введения, двух глав, заключения и списка использованных источников.

# 1. Теоретические основы феномена информационной войны

## 1.1. Понятия пропаганды, информационной и психологической войны

Согласно словарю Мерриама-Уэбстера, понятие «информация» - это «знание, полученное в результате исследования, изучения или обучения» [1]. И наоборот, термин «дезинформация» - это «ложная информация, преднамеренно и часто тайно транслируемая (например, путем распространения слухов) с целью повлиять на общественное мнение или скрыть истину» [2]. Эти определения являются продуктом многовекового человеческого опыта распространения информации со времен наскальных рисунков до письменной, устной и, в конечном счете, электронной передачи информации.

В современной реальности использование информации или дезинформации в качестве инструмента ведения политического противостояния берёт свои истоки с конца 400-х годов до нашей эры в трудах знаменитого военного стратега Сунь-цзы. В его работе «Искусство войны» одним из главных постулатов было то, что «всякая война есть обман» [3]. Противника нужно постоянно сбивать с толку самыми изощрёнными проявлениями хитрости, как то, например: если в стане врага царит гармония, необходимо посеять раздор, тем самым обращая эмоции оппонента в свою пользу; при наличии особенной информации и ресурсов нужно делать вид, что их нет, как бы принижая себя, а если же никаких дополнительных средств не имеется, наоборот, открыто заявлять, что они есть, устрашая. Таким образом, можно говорить о том, что Сунь-цзы был одним из первых военных стратегов, резюмировавших предпосылки информационного и психологического воздействия на противника, что в середине XX века было известно под термином «психологическая война».

Пропаганда стала играть значительную роль, когда большинство населения в странах европейской цивилизации стало грамотным. Тогда же

появились средства связи, способные донести информацию до широких слоев населения, как, например, газеты и журналы, вышедшие в массовый тираж, тогда как еще в середине XIX века их печатали всего несколькими тысячами экземпляров. Плакаты, открытки, листовки и брошюры, а также делавшая первые шаги кинематография также стали частью массовых коммуникаций. Печатные тиражи книг были еще невелики, поэтому книги в основном влияли на интеллектуальную часть общества [4].

Термин «пропаганда» получил широкое распространение ещё во времена Первой мировой войны, задолго до появления таких понятий, как «информационная война» и «психологическая война», и примерно в то же время пропагандистские технологии прочно вошли в практику СМИ. Стоит отметить, что особенно активно продвигали и развивали пропагандистские и информационные теории в военное время исследователи из Великобритании [4]. Именно государства Антанты в лице Великобритании и Франции в первую очередь вели беспрецедентную пропаганду, направленную против врага: в период с 1914 по 1918 годы в населённых пунктах, а также в стане вооружённых сил Германии распространялось около 30 миллионов листовок, газет и брошюр.

После Первой мировой войны печатные издания книг увеличились, а вместе с ними и сфера их влияния. Начиная с 1920-х годов появился такой мощный инструмент массовой коммуникации, как радио. Он стал важным инструментом воздействия на малограмотное население и вскоре распространился по всему миру. В то же время кинематограф также стал важным инструментом массовой коммуникации. С середины 20 века телевидение обретало всё возрастающую роль как средства коммуникации и до сих пор остается мощнейшим инструментом пропаганды. Начиная с 1980-х годов особенно важным инструментом связи и передачи информации стал Интернет, а с начала 21 века – социальные сети.

Действительно, целью любого производителя информации является определение и формирование взглядов отдельных лиц и групп желаемым для

себя образом, что непосредственно связано с понятием пропаганды. Согласно официальной дефиниции Британской энциклопедии, «пропаганда» - это распространение информации - фактов, слухов, полуправды или лжи – призванное повлиять на общественное мнение [5]. Однако это определение представляется слишком общим. Рациональнее определить «пропаганду» как специально подготовленную информацию, направленную на распространение и продвижение определенных взглядов и поведения по отношению к определённым событиям у отдельных лиц и групп.

Можно сказать, что основная разница между пропагандой и информационной войной состоит в том, что информационная война ведётся, в большинстве случаев, параллельно с конвенциональной, гибридной или любой другой войной, а пропагандистские стратегии могут внедряться на постоянной основе. Пропаганда подчеркивает положительный имидж «наших», а информационная война акцентирует внимание на отрицательной сущности «иных». Информационная война представляет собой пропагандистские кампании, призванные сформировать образ врага и уверить граждан своей страны в правоте государственной позиции, а также в необходимости придерживаться определенных взглядов и стремиться к выполнению установленных задач. В подобного рода кампаниях определённые массивы информационного контента искажаются, а правдивая информация проходит через многоступенчатый анализ и редактуру в соответствии с целями, преследуемыми операциями информационной войны [4].

Пропаганда и информационная война наиболее эффективны в государствах с сильными авторитарными режимами, так как большинство СМИ там находятся под контролем правительства, жёстко цензурирующего и координирующего то, как СМИ формируют желаемый положительный или отрицательный образ у большей части населения. А поскольку такой режим передачи информации существует не только во время активных военных действий, но и в мирное время, то переход на режим информационной войны осуществляется быстро и практически незаметно. В демократических странах

целенаправленная пропаганда на государственном уровне применяется только в военное время и ведется в форме информационной войны. В такие времена вводится цензура освещения военных действий и внутренних событий [6].

Не только правительство, но и неправительственные организации, частные лица и многие другие акторы предпринимают попытки влияния на СМИ, чтобы создать образ врага с противоположной стороны поля противостояния. Воздействие осуществляется через финансирование СМИ и конкретных информационных проектов, а также путём введения со стороны государства нового законодательства в виде налоговых льгот для СМИ, обслуживающих военные нужды, а значит, участвующих в информационной войне. В то же время, поскольку сохраняется свобода слова, пусть и ограниченная условиями военного времени, внутри общества возможны критические взгляды на навязываемые властью образы. Их принятие не имеет такой тотальности, как в тоталитарных государствах [4].

Если говорить о современной аудитории в развитых демократических странах или, по крайней мере, о наиболее прогрессивной её части, формирующей общественное мнение, то надо учитывать, что сами слова «пропаганда» и «информационная война» несут в себе ощутимую негативную коннотацию. Именно по этой причине пропаганда в таких странах носит более сдержанный и менее тоталитарный характер. В СМИ допустимы дискуссии и выражение точек зрения, противоположных официальной правительственной позиции. Пропаганда в таких странах может быть эффективной лишь при условии хотя бы поверхностной объективности и свободы критики [4].

Информационные технологии, появившиеся в конце XX века, изменили мировоззрение и затруднили интерпретацию получаемой информации. Это привело к быстрому и неконтролируемому увеличению объема информационных потоков и резко снизило качество информации с точки зрения возможностей проверки степени её достоверности. В настоящее время практически невозможно произвести необходимую критическую и объективную оценку информации. Даже если исследователь или обычный

потребитель получает информацию, которую он, например, считает новой, это не обязательно так, потому что аналогичные результаты могли быть получены и использованы другими исследователями и потребителями информации [4].

Говоря о понятии психологической войны — это спланированное тактическое использование пропаганды, угроз и других небоевых приемов во время войн, угроз войны или периодов геополитических волнений с целью ввести в заблуждение, запугать, деморализовать или иным образом повлиять на мышление или поведение противника. Психологическая война обычно использует пропагандистские стратегии для воздействия на ценности, убеждения, эмоции, рассуждения, мотивы или поведение своих целей. Мишенями таких пропагандистских кампаний могут быть правительства, политические организации, правозащитные группы, военнослужащие и гражданские лица.

Хотя это может показаться современным феноменом, психологическая война так же стара, как и сама война. Например, в битве при Пелузее в 525 году до нашей эры персидские войска держали кошек в заложниках, чтобы получить психологическое преимущество над египтянами, которые из-за своих религиозных убеждений отказывались причинять вред этим животным [7].

Вождь Монгольской империи 13 века нашей эры Чингисхан, чтобы численность его войск казалась больше, чем была на самом деле, приказывал каждому солдату нести ночью три зажженных факела. Могучий хан также изобрел стрелы с зазубринами, которые свистели в воздухе, наводя ужас на его врагов. И, возможно, одним из самых экстремальных проявлений тактики запугивания являлся эпизод, когда монгольские армии катапультировали отрубленные человеческие головы через стены вражеских деревень, чтобы напугать жителей [7].

Современная тактика психологической войны впервые была применена во время Первой мировой войны. Технологические достижения в области электронных и печатных средств массовой информации облегчили правительствам распространение пропаганды через массовые тиражи газет. На

поле боя достижения авиации позволили сбрасывать листовки в тыл врага, а для ведения пропаганды были разработаны специальные несмертельные артиллерийские снаряды.

Во время Второй мировой войны как державы Оси, так и союзные державы регулярно использовали так называемые психологические операции. Приход Адольфа Гитлера к власти в Германии был во многом обусловлен пропагандой, направленной на дискредитацию его политических противников. Его яростные речи пробуждали в слушателях национальную гордость и одновременно убеждали народ обвинять других в экономических проблемах Германии.

Ведение психологических операций посредством радиовещания достигло пика во время Второй мировой войны. Знаменитая японская «Токийская роза» транслировала музыку с ложной информацией о японских военных победах, чтобы обескуражить союзные войска. Германия использовала аналогичную тактику в радиопередачах «Вылазки оси» [7].

Холодная война почти закончилась, когда президент США Рональд Рейган публично обнародовал подробные планы создания высокоразвитой противоракетной системы Стратегической оборонной инициативы (СОИ) «Звёздные войны», способной уничтожить советские ядерные ракеты до того, как они вновь войдут в атмосферу. Независимо от того, действительно ли могла быть построена какая-либо из систем «Звездных войн» Рейгана, советский президент Михаил Горбачев верил в реальность угрозы [7]. Столкнувшись с осознанием того, что затраты на противодействие американским достижениям в области систем ядерного оружия могут обанкротить его правительство, Горбачев согласился возобновить переговоры эпохи разрядки, результатом которых стали долгосрочные договоры о контроле над ядерными вооружениями.

В качестве ещё одного из наиболее известных примеров ведения «психологической войны» нельзя не отметить действия Соединенных Штатов, ответивших на теракты 11 сентября 2001 года началом войны в Ираке

массированной военной кампанией «шок и трепет», призванной сломить волю иракской армии к борьбе и защитить диктаторского лидера страны Саддама Хусейна. Вторжение США началось 19 марта 2003 года с двухдневных безостановочных бомбардировок столицы Ирака Багдада. 5 апреля силы коалиции США и союзников, столкнувшись лишь с символическим сопротивлением иракских войск, взяли под контроль Багдад. 14 апреля, менее чем через месяц после начала вторжения в Ирак, США объявили о победе в войне в Ираке [7].

Признаётся, что термин «психологическая война» был введен в практику СМИ английским военным теоретиком и историком Дж. Фуллером в 1920 г. В своей книге «Танки в Великой войне, 1914–1918 гг.» он писал: «…этот метод навязывания воли одного человека другому может, в свою очередь, быть заменен чисто психологической войной, при которой даже не применяется оружие, не ищутся поля боя и не ставится целью гибель людей или увечий; но вместо этого совершается развращение человеческого разума, затемнение человеческого ума и разложение нравственной и духовной жизни одного народа влиянием воли другого» [6].

Одной из первых работ по исследуемой теме стала книга американского политолога и психолога Пола Лайнбаргера «Психологическая война», где автор обобщил свой опыт работы в пропагандистских учреждениях США, занимающихся психологической войной. Автор утверждал, что практически все методы, формы и технологии психологической войны в США были разработаны подразделениями офицеров и аналитиков, имевших образование в области психологии человека, политической психологии, прикладной психолингвистики, психологии пропаганды и массовых коммуникаций.

В своей книге 1949 года «Психологическая война против нацистской Германии» бывший оперативник ЦРУ Дэниел Лернер подробно описывает американскую военную кампанию Skyewar Второй мировой войны. Лернер разделяет пропаганду психологической войны на три категории или же вида: белая пропаганда, в которой информация правдива и лишь умеренно предвзята,

а также приводится источник транслируемой информации; серая пропаганда, где информация в основном правдива и не содержит никаких деталей, которые можно было бы опровергнуть, однако, никаких источников не приводится; черная пропаганда: буквально «фальшивые новости», информация является ложной и приписывается источникам, не ответственным за ее создание.

Хотя серые и черные пропагандистские кампании часто оказывают самое непосредственное воздействие, они также несут в себе наибольший риск. Рано или поздно целевая аудитория идентифицирует информацию как ложную, тем самым дискредитируя источник. Как писал Лернер: «Доверие - это условие убеждения. Прежде чем заставить человека делать то, что вы говорите, вы должны заставить его поверить в то, что вы говорите» [7].

Возвращаясь к феномену информационной войны, стоит ещё раз подчеркнуть, что как «психологическая война» и «пропаганда», это не новое явление. В битве при Фермопилах в 480 году до нашей эры персидский правитель Ксеркс использовал тактику запугивания, чтобы сломить волю греческих городов-государств. Александр Македонский использовал культурную ассимиляцию, чтобы подавить инакомыслие и сохранить завоеванные земли. Также уже упомянутые древние стратеги Сунь-цзы и его «Искусство войны» помогли заложить основу стратегии информационной войны в наше время.

«Война» может быть определена широко и включать в себя практически любую деятельность, предпринятую одной группой для ослабления или уничтожения другой. Однако применение приставки «война» к экономике, политике или социальным вопросам – лишь отвлекающая гипербола. В любой другой области — воздушной, морской или наземной — война четко определяется как связанная с вооруженными конфликтами, насилием и разрушениями. Информационная война ничем не должна отличаться.

Американский физик Томас Рона ввел термин «информационная война» в 1976 году. Он определил, что информационная война возникает из-за зависящих от информации систем вооружения и военных операций,

контролируемых на огромном боевом пространстве в режиме реального времени. В исследовании «Системы вооружений и информационная война» Роны для Главного управления военных оценок Министерства обороны США отмечается необходимость признания и использования информационной войны как непосредственно связанной с материальным аспектом боевой готовности и военных операций [7].

Предсказания Роны об информационной войне 45-летней давности стали реальностью. Информационные технологии, определяющие и интерпретирующие боевое пространство, переплетены и неразрывно связаны с физическим, материальным миром. Информационные противостояния в боевом пространстве пересекаются с операциями в наземной, морской, воздушной и космической областях, точно так же, как эти области пересекаются друг с другом.

Информационная война, определяемая ниже уровня вооруженного конфликта, представляет собой комплекс военных и правительственных операций по защите и использованию информационной среды. Независимо от того, нападают ли на правительственные учреждения, политическое руководство или средства массовой информации с целью повлиять на общественное мнение или заставить лиц, принимающих решения, предпринять определенные действия, в конечном счете целью информационной войны является человеческое сознание [8]. По этой причине информационную войну иногда называют операциями убеждения, влияния или психологической войной, что представляет верным лишь отчасти, учитывая, что психологическая война является одним из видов информационной войны, о чём речь пойдёт позже.

Однако информационная война не всегда может включать в себя решения принудительного характера; скорее, она может быть частью политики «разделяй и властвуй» - стратегии, нацеленной на дестабилизацию гражданского общества, с целью создать паралич механизма принятия решений. Лица, принимающие решения в этом случае, постоянно подвергаются

бомбардировке противоречивыми сообщениями, и не имеют при этом легкодоступных средств распознать истину. В отсутствие достоверной информации и при усилении противодействия со стороны фракций по обе стороны вопроса, лица, принимающие решения, могут оказаться неспособными действовать. Это информационный эквивалент того, что Карл фон Клаузевиц назвал «туманом и трением» войны. Туман войны относится к неопределенности в ситуационной осведомленности, испытываемой участниками военных операций, в то время как трение является побочным продуктом этого тумана [8].

Информационная война также может быть прелюдией к вооруженному конфликту, подготовкой поля боя, предшествующей развертыванию сил. Информационные операции создают условия, чтобы заручиться поддержкой местных жителей, «завоёвывая сердца и умы», чтобы увеличить шансы на успешную кампанию. С другой стороны, информационная война может быть самоцелью, процессом, посредством которого нации получают конкурентные преимущества друг перед другом без применения силы.

Хотя информация признается элементом национальной власти, информационная война является относительно обтекаемым понятием, научным сообществом до сих пор не было принято для него единого определения. Также этот термин остаётся неопределённым и Министерством обороны, что приводит к множеству его интерпретаций.

Представляется возможным определить информационную войну как интегрированное использование средств радиоэлектронной борьбы, компьютерных сетевых операций, психологических операций, военного обмана и обеспечения безопасности операций в сочетании с определенными вспомогательными и связанными с ними возможностями, чтобы влиять, нарушать, искажать или узурпировать враждебное человеческое и автоматизированное принятие решений, защищая при этом собственное. То есть, в более широком смысле это любые действия по отрицанию, использованию, искажению или уничтожению информации, касающейся

противника; защиты себя от подобных действий, а также использование собственных военных информационных функций [8].

Эти определения предполагают, что информационная война представляет собой совокупность методов, использующих информацию для достижения стратегического или конкурентного преимущества над противником. Кроме того, приведенные выше определения также предполагают, что получение такого конкурентного преимущества требует обеспечения адекватной защиты от информационных операций противника. Следовательно, укрепление систем безопасности будет играть важную роль в стремлении получить преимущество над противником на арене информационной войны.

Итак, из вышеизложенного следует вывод о том, что информационная война - это стратегия использования информации для достижения конкурентного преимущества, включающая наступательные и оборонительные усилия. Будучи формой политической войны, информационная война является средством, с помощью которого нации достигают стратегических целей и продвигают цели внешней политики. Оборонительные усилия включают обеспечение информационной безопасности, в то время как наступательные усилия включают информационные операции. Информационную войну иногда описывают как «кампанию дезинформации», но дезинформация - это лишь одна из тактик или же методов, используемых в информационных операциях. Пропаганда – инструмент информационной войны, а психологическая война – один из её видов.

### 1.2. Виды информационной войны

Вид информационной войны есть способ её ведения, выражающийся через структуру действий, связанных с происходящими в нём процессами. Это означает, что вид информационной войны является особым признаком, качественно отличающим его от других форм.

При изучении видов информационной войны мы обратились к работам Мартина Либицки - одного из первых теоретиков в данной области. По словам Либицки, информационная война имеет следующие виды реализации: 1) кибервойна; 2) хакерская война; 3) психологическая война; 4) разведывательная война; 5) радиоэлектронная борьба; 6) информационно-экономическая война; 7) командно-административная война [9].

Все эти виды взаимосвязаны и не являются полностью обособленными.

Представляется важным акцентировать особенное внимание на таком виде информационной войны, как кибервойна, так как нередко эти понятия ошибочно отождествляются. Согласно Либицки, кибервойна состоит из информационного терроризма, семантических атак, войны стимулов и войны Гибсона [10].

Информационный терроризм — это информационное воздействие с целью реализации интересов отдельно взятых террористов или террористических группировок. Семантические атаки аналогичны хакерской войне, за исключением того, что в хакерской войне конечной целью является вывести систему из строя, а в данном случае система даёт реалистичные ответы, поэтому вы не знаете, что она подверглась атаке. Война стимулов — это имитация реальной войны. Симуляция продемонстрирует, кто выиграет физическую войну. Последней областью кибервойны является война Гибсона — это виртуальная битва между двумя сторонами. Либицки также отмечает, что глобальная инфраструктура всё ещё недостаточно развита для этого типа войны [10].

Согласно совместной публикации 3-12 Министерства обороны США, киберпространство определяется как «глобальная область в информационной среде, состоящая из взаимозависимой сети информационно-технологических инфраструктур и резидентных данных, включая Интернет, телекоммуникационные сети, компьютерные системы и встроенные процессоры и контроллеры» [11]. Большая часть современной информационной войны проводится в киберпространстве, что заставляет многих ассоциировать

информационную войну с кибербезопасностью. Однако в рамках международных отношений операции информационной войны и киберпространства являются различными доктринальными видами деятельности. Операции в киберпространстве могут быть использованы для достижения стратегических целей информационной войны; например, наступательная кибератака может быть использована для создания психологического воздействия на гражданское население. Иностранная держава может использовать кибератаки для влияния на принятие решений и изменения поведения, например, кибератаки на Sony, совершенные Корейской Народно-Демократической Республикой (КНДР) в конце 2014 года [8]. Кибероперации могут проводиться и для других целей, таких как отключение или отказ в доступе к линиям связи противника.

Анонимность, обеспечиваемая киберпространством, является идеальной «боевой ареной» для проведения тайных информационных операций. Кроме того, информационная война может происходить и за пределами киберпространства.

Хотя между информационной войной и кибервойной есть некоторое сходство, масштабы этих двух областей существенно различаются. Информационная война является более старым явлением, чем кибервойна, и на протяжении всей истории была фундаментальной частью обычных войн. С другой стороны, кибервойна — относительно новое явление, потому что она возникла с изобретением интернета и компьютеров, в отличие от ряда операций информационной войны, существовавших задолго до этого.

Прежде всего, в сфере информационных операций именно информация используется как оружие против противника. В связи с этим Объединенный комитет начальников штабов США выделил три отдельных элемента информационных операций: они включают физическую, когнитивную и информационную сферы [12]. Перечень действий, которые могут осуществляться в сфере информационного противоборства, достаточно обширен и включает в себя распространение пропаганды, «фейковых новостей»

или дезинформации через СМИ и социальные сети. Это также включает распространение вредоносных программ и вирусов, а также атаки по типу «отказ в обслуживании» («DDoS») на системы военного управления противника [12].

С другой стороны, кибервойна включает в себя использование только Интернета и компьютеров как средства получения стратегического конкурентного преимущества над противником. Кибервойна основана на DDoS-атаках, компьютерных вирусах, взломе и атаках вредоносных программ на стратегически важные компьютерные системы противника [12]. Таким образом, информационная война — это более широкая сфера, включающая в себя печатные и электронные СМИ, компьютеры, программное обеспечение, слежку и шпионаж, в то время как масштабы кибервойны ограничены Интернетом и компьютерами.

Хакерская война — это также один из видов информационной войны, которую чаще всего ведут отдельные лица. Хакерская атака обычно направлена на перегрузку и изменение содержимого атакуемого веб-сайта. Благодаря своим функциональным и физическим характеристикам компьютерные системы представляют собой идеальную цель для злоумышленников [13]. Использование хакерской войны в значительной степени зависит от количества используемых компьютеров и количества пользователей Интернета. Степень интеграции компьютерных сетей обратно пропорциональна эффекту хакерской войны [10].

Психологическая война уже детально рассматривалась в нашем исследовании. Это запланированные операции по доведению выбранной информации до аудитории, чтобы повлиять на их эмоции, мотивы, объективное мышление и, в конечном счете, на поведение организаций, групп и отдельных лиц.

Разведка — это деятельность, направленная на поиск целей, оценку боевых действий, предотвращение неожиданностей и т. д. Первичные источники разведки можно разделить на разные категории: агентурная

разведка, сигнальная разведка, техническая разведка и другие [13]. Либицки утверждает, что разведывательная война возникает, когда разведданные вводятся непосредственно в ход операции (определение целей и оценка боевых повреждений), а не используются в качестве исходных данных для общего управления и контроля [10]. Разведывательная война в контексте информационной войны играет скорее вспомогательную роль. К примеру, при наличии качественной разведслужбы можно понять, какие именно части информационной сети нужно уничтожить, чтобы дестабилизировать механизмы принятия решений в случае ведения командно-административной войны. Также невозможно защищаться от разведслужб, не имея понятия о том, как разведданные собираются противником.

Ещё один вид информационной войны - радиоэлектронная борьба - это комплекс боевыех действий, в которых электронные и другие средства непосредственно воздействуют на радиоэлектронные средства и системы противника, а также на боевые системы и средства поражения, основанные на использовании электроники [13]. Профессор К.Шлехер в своей работе «Electronic Warfare in the Information age» определяет радиоэлектронную войну как «военные действия, направленные на контроль электромагнитного спектра» [14]. Согласно исследованию факультета электротехники Белградского университета, радиоэлектронная борьба представляет собой комплекс военных действий, основной целью которых является контроль над электромагнитным пространством, его доменом [13]. Для достижения поставленной цели применяются мероприятия, имеющие наступательный характер – радиоэлектронные атаки, и оборонительный характер - радиоэлектронная защита.

Радиоэлектронная атака — это часть радиоэлектронной борьбы, предполагающая использование электромагнитной энергии или направленной энергии для атаки с целью ослабления, нейтрализации или уничтожения боевых потенциалов противника [13]. Радиоэлектронная защита - часть радиоэлектронной борьбы, охватывающая мероприятия, направленные на

защиту своих людей и средств от воздействия средств радиоэлектронной борьбы противника, а также от непреднамеренных излучений собственных передатчиков, способных ухудшить, нейтрализовать или уничтожить боевые возможности собственных сил. Радиоэлектронное обеспечение - часть радиоэлектронной борьбы, включающая в себя деятельность по обнаружению, идентификации и местонахождению источников преднамеренного или непреднамеренного излучения электромагнитной энергии для обнаружения действий противника, обнаружения местоположения целей, планирования и осуществления поддержки радиоэлектронной борьбы. и другие тактические действия [14]. Информация о противнике, собранная с помощью механизмов радиоэлектронной борьбы, имеет значительный разведывательный потенциал, и тогда радиоэлектронную борьбу можно рассматривать как разведывательную войну. Однако разведывательная борьба заключается в функции планирования и ведения радиоэлектронной борьбы и, в частности, формирования картины поля боя.

Понятие «экономико-информационная война» до сих пор не имеет чёткого определения, но ясно, что эта форма информационной войны ориентирована на информацию, имеющую экономическое значение для конфликтующих сторон. Это может представлять собой сведения о различных контрактах, стратегических разработках компании, внутренней структуре организации, маркетинговые и производственные планы, инвестиции и многое другое [13]. Очевидно, что в глобальном контексте постоянно присутствует «конфликт» экономических и разведывательных служб вокруг конфиденциальной информации, которая будет использована против конкурентов в интересах компании. Этот «конфликт» по существу является экономическим (или промышленным) шпионажем.

Последний из видов информационной войны – командно-административная война. Официальное определение Министерства обороны США по боевым действиям в командовании и управлении звучит так: «Командно-административная война — это военная стратегия, которая

применяет информационную войну на поле боя, чтобы отделить командную структуру противников от подразделений, которыми они командуют» [10]. Обезвреживание может производиться путем повреждения командного пункта или связи, в зависимости от различных тактических и стратегических целей. Либицки считает, что это гораздо важнее, чем найти физическое местонахождение командира, обнаружившего командный пункт [10]. Атака командных позиций, особенно своевременно скоординированная, может иметь исключительные оперативные последствия. В большинстве ситуаций командный пункт является узлом во всей структуре противника и его ликвидация редко упускается. Его можно разрушить классическими бомбами, а также перебоями в электроснабжении, электромагнитными помехами, компьютерными вирусами, прерыванием связи и т. д. Командно-административная война может вестись как наступательно, так и оборонительно. На основании вышеизложенного можно сделать вывод, что цель командно-административной войны состоит в том, чтобы ухудшить или разрушить потенциал противников для управления и контроля, в то же время защищая свои собственные потенциалы от подобной деятельности.

Информационная война — это любое организованное использование или манипулирование информацией или знаниями, направленное на получение преимущества в борьбе с противником. Вопрос о том, применяется ли использование или манипуляция к мыслительным процессам оппонента или к программному и аппаратному обеспечению, составляющему информационные системы оппонента.

### 1.3. Формы, методы и цели информационной войны

Существует две основных формы информационной войны: информационная война, ведущаяся извне, а защитой от таких атак могут быть брандмауэры, физическая изоляция и шифрование; информационная война изнутри - защита от инсайдеров, связана с личной безопасностью и рабочими

процедурами [15]. Информационные операции извне в масштабах одного государства предполагают кибератаки со стороны государственных и негосударственных иностранных акторов, хакерские операции, взломы систем и т.п. Информационные операции, ведущиеся изнутри, соответственно, представляют, к примеру, кампанию дезинформации со стороны радикальной оппозиции, ведущуюся путём распространения заведомо ложных сведений о ведущих политических деятелях страны. Воздействуя непосредственно на население психологически и эмоционально, злоумышленники манипулируют сознанием масс, тем самым подрывая авторитет государства и доверие к нему со стороны общества. Говоря в этом контексте о внутренних рисках кибербезопасности можно упомянуть также о возможности политического шпионажа со стороны завербованных иностранными государствами сотрудников, имеющих доступ к основополагающим системам безопасности. Такие шпионы могут передавать засекреченные сведения государственной важности или вести иного рода подрывную деятельность.

Существует пять основных методов информационной войны [15]:

Первым из методов можно назвать атаку на данные. Атаки на данные происходят, когда противник вводит данные и таким образом манипулирует информационной системой. Примерами являются повреждение файлов, глушение радиопередач данных, распространение вводящей в заблуждение пропаганды и рассылка спама (отправка больших объемов входных нерелевантных данных). Следует признать, что кампании информационной войны не всегда требуют сложных технологий. Кампании по дезинформации можно проводить многими нехитрыми способами, и человеческий фактор, такой как принятие решений, всегда имеет основное значение в операциях. Медиа-сектор является одним из главных полей битвы. Психологические операции могут быть основаны на изучении общественного мнения и анализе в качестве основы для индивидуальных сообщений.

Нередко атаки на данные политически мотивированы и направлены на манипулирование политической ситуацей. Известным случаем кражи данных

является скандал с Cambridge Analytica, когда один из членов правления фирмы получил доступ к данным 50 млн. пользователей социальной сети Facebook. Эти данные использовались для президентской предвыборной кампании Дональда Трампа в 2016 году. Согласно отчетам расследования, доступ к данным осуществлялся через онлайн-приложение, созданное независимым исследователем и преподавателем Кембриджского университета Александром Коганом. Приложение-опросник стало известно среди пользователей Facebook, и любой, кто получил доступ к приложению и использовал его для проверки личности, непреднамеренно передал свои данные и данные друзей в Facebook приложению Когана. Позднее Коган поделился этими данными с Cambridge Analytica. Прежде всего, это были данные граждан США и Великобритании. Это произошло в 2015 году, когда политическая команда Дональда Трампа была занята предвыборной кампанией, а один из членов команды, Стив Бэннон, оказался членом совета директоров Cambridge Analytica. Так, он использовал данные приложения Когана для предвыборной кампании Трампа и, следовательно, политическая команда обрабатывала содержание речей Трампа, а также многих других нарративов предвыборной кампании в соответствии с интересами и предпочтениями людей, чьи данные были доступны [16]. Следовательно, попытка повлиять на результат президентских выборов была достигнута путем кражи личных данных тысяч граждан США без их разрешения. Было высказано предположение, что Россия могла поддержать кражу данных и помочь политической команде Трампа, однако по результатам расследований, фактических доказательств вмешательства России не было выявлено. Как итог, помимо того, что компания Facebook понесла колоссальные финансовые и репутационные потери в связи с падением акций и доверия пользователей, «Закон о честной рекламе» стал более строго применяться на всей территории Соединенных Штатов. Этот закон обязывает все компании, занимающиеся социальными сетями и программным обеспечением, делиться содержанием своей политики и всеми сопутствующими действиями с Государственным департаментом США в

отношении запуска любых видов приложения, занимающегося сбором данных отдельных лиц, и которое потенциально может быть использовано в политических целях.

Одним из наиболее распространённых методов ведения информационной войны являются программные атаки. Они направлены на выполнение функций, как внедрение компьютерных вирусов, троянских коней, логических бомб и лазеек, которые позволяют враждебной стороне иметь беспрепятственный доступ к системе. Бэкдоры в программном обеспечении могут быть направлены на атаку встроенных механизмов защиты и безопасности. Микрочипы могут иметь запрограммированные заранее слабые места или иметь скрытые дополнительные функции, которые могут быть использованы противником в конфликте (чипирование).

Как пример программной атаки широко известен Stuxnet - это компьютерный червь, который первоначально был нацелен на ядерные объекты Ирана, вследствие чего серьёзно нарушил систему производства ядерного оружия в Иране, и с тех пор мутировал и распространился на другие промышленные и энергетические объекты. Оригинальная вредоносная атака Stuxnet была нацелена на программируемые логические контроллеры (ПЛК), используемые для автоматизации машинных процессов. Он вызвал шквал внимания со стороны средств массовой информации после того, как был обнаружен в 2010 году, потому что это был первый известный вирус, способный повредить аппаратное обеспечение, а также потому, что он, по-видимому, был создан Агентством национальной безопасности США, ЦРУ и израильской разведкой. Хотя власти Ирана не обнародовали конкретных подробностей о последствиях атаки, в настоящее время считается, что червь Stuxnet уничтожил 984 центрифуги по обогащению урана. По современным оценкам, это привело к снижению эффективности обогащения на 30%, развитие ядерной программы страны на значительный период времени было парализовано [17]. Захватив и нарушив промышленные процессы в масштабном секторе суверенного государства, Stuxnet стал поистине

наступательным кибероружием, увеличив растущий потенциал и готовность государств и спонсируемых государствами групп участвовать в кибервойне.

Также существует такой метод как хакерские атаки (или взлом, который является криминальным аспектом) — это несанкционированный вход в информационную систему с целью взаимодействия с её функцией, чтобы спровоцировать обман, кражу, мошенничество, уничтожение и другие виды вреда. Программное обеспечение может использоваться тайно для создания преднамеренных излучений, которые обходят обычные механизмы безопасности. Это может быть использовано для коммерческого и национального шпионажа или для обеспечения соответствия программного обеспечения.

В апреле и мае 2007 года хакеры развязали волну кибератак, которые нанесли ущерб десяткам правительственных и корпоративных сайтов в Эстонии, одной из самых проводных стран Европы. Эстонские власти предположили, что скоординированные хакерские атаки на правительственные учреждения и банки были организованы Кремлем - обвинение, которое Москва отвергла. Онлайн-атака последовала за решением Эстонии перенести советский мемориал Второй мировой войны из центра Таллина 27 апреля 2007 года, что вызвало яростные протесты российского правительства и беспорядки среди этнического русского меньшинства Эстонии.

Метод «отказ в обслуживании (DDoS)», который по сути является потерей доступа, уже нами частично затрагивался. Такого рода атаки просты в исполнении и от них сложно защититься. Интернет-атаки демонстрируют, что это может повлиять на функционирование огромных систем.

Примером одной из наиболее крупных DDoS-атак является случай, произошедший 21 октября 2016 года. Dyn, крупный поставщик услуг доменных имен (DNS), подвергся атаке потока трафика в один терабит в секунду, который в то время представлял собой новое рекордное значение для DDoS-атаки. Цунами трафика вывело сервисы Dyn из строя, сделав недоступными ряд крупных сайтов, включая GitHub, HBO, Twitter, Reddit, PayPal, Netflix и Airbnb

[18]. Ботнет Mirai был ответственен за крупнейшие атаки того времени, и самым примечательным в них на 2016 год была публикация исходного кода в открытый доступ, что позволяло любому пользователю, обладающему даже самыми минимальными навыками в области информационных технологий, создать ботнет и организовать атаку типа "Отказ в обслуживании" без особых усилий.

Завершают список физические атаки — это попытки физически разрушить систему. Примерами являются использование бомб; создание различных вредных сред, таких как электромагнитные импульсы, микроволновые печи высокой мощности и другие среды направленной энергии; или создание электромагнитного терроризма. Высокомощное микроволновое оружие может излучать повторяющиеся импульсы высокой мощности в узкой полосе частот, сконцентрированной на частоте от нескольких сотен МГц до нескольких ГГц. Такое обычно высокотехнологичное оружие может вызвать «повреждение входной двери» оборудования. Мощное импульсное сверхширокополосное оружие может излучать короткие повторяющиеся импульсы (обычно длительностью в сотни пикосекунд), распределяющие мощность по очень широкому спектру. Оружие может быть низкотехнологичным, дешевым и, вероятно, вызовет «нарушение черного хода». Коммерчески доступны устройства непрерывного глушения, которые могут нарушить работу глобальной системы позиционирования (GPS) или услуг мобильной связи; существуют и другие типы радиочастотного и электромагнитного импульсного оружия [14].

При детальном изучении нами было принято решение создать шкалу опасности, согласно которой можно расположить методы ведения информационных войн в порядке их вредоносности – от наиболее к наименее опасному. Это позволит максимально объективно определять степень угрозы и оценивать риски при анализе конкретных кейсов. За основу распределения взят фактор степени вреда, причиняемого общественным отношениям и

государственным интересам. Соответственно, самый вредоносный метод – тот, что оказывает негативное воздействие на обе сферы.

В нашей шкале существует две градации: первая описывает дефолтное состояние информационной войны, взятое в отрыве от нынешних реалий и международной обстановки (физические атаки – хакерские атаки – программные атаки – атаки на данные – DDoS-атаки); вторая основывается на текущих данных и представляется наиболее актуальной (атаки на данные – физические атаки – хакерские атаки – программные атаки – DDoS-атаки).

В первом случае физические атаки занимают лидирующую позицию на основании того, что наносят вред не только информационной системе и ресурсам, но и представляют угрозу обществу. Однако на сегодняшний день вредоносность физических атак отходит на второй план, уступая место атакам на данные. Изначально атаки на данные рассчитаны прежде всего на мало осведомлённых в фактическом информационном состоянии людей, но, несмотря на это, они в большей степени воздействуют на состояние общественных отношений, поскольку могут обеспечить манипулирование сознанием, повлечь массовые беспорядки, экстремистские выступления, в том числе и крайние формы экстремизма – террористические акты. Это малозатратный, но высокоэффективный метод ведения информационной войны. В этой связи сложно говорить, что первый вид градации вредоносности методов во главе с физическими атаками соответствует текущему состоянию общества, так как общество по своей сути не статично и постоянно меняется. Слухи, домыслы и «грязная пропаганда» всегда причиняли больше вреда, чем средства комплексного воздействия, как средства связи и т.п., и как доказательство мы наблюдаем нынешние реалии, в которых подобные средства позволяют изолировать от всего мира целую страну. Данный метод ведения информационной войны становится максимально опасным и требует оперативного реагирования со стороны государства.

Следующими по вредоносности являются хакерские атаки, так как их последствия включают причинение вреда охраняемым законом интеерсам

государства и общества, а сами атаки преследуются в уголовном порядке. Далее – программные атаки, потому что среди прочих угроз программная атака воздействует в меньшей степени на физические объекты, а в большей блокирует нормальную работу программного обеспечения систем и сетей связи и данных. Завершают классификацию DDoS-атаки. Несмотря на то, что общество и государство придаёт значительное внимание указанной категории информационных воздействий, следует подчеркнуть, что в большей степени характер причиняемого подобного рода атаками вреда, влияет на жизнеспособность информационных ресурсов, и в Российской Федерации государство это преследует как в уголовном, так и в административном порядке.

Вышеизложенный материал также доказывает, что основными целями атак информационных войн являются: эксплуатация – использование информации оппонента в своих целях; обман – чтобы манипулировать информацией противника и поддерживать его деятельность; нарушение или отказ в обслуживании – чтобы вывести систему из строя на некоторое время или сделать её ненадежной; и, наконец, уничтожение - нанесение вреда системе таким образом, что она больше не может работать [15].

Как итог очевидно, что информация - это и ресурс, и оружие. Когда вражеские субъекты одновременно действуют в космосе, киберпространстве и по всему электромагнитному спектру, реагирование в реальном времени становится проблемой на поле боя, а добавление космоса и киберпространства в качестве областей боевых действий экспоненциально расширило и значительно усложнило ведение информационных войн и связанных с ними информационных операций.

Никакая информационная война никогда не была ключевым фактором победы одной из сторон в вооруженном конфликте, хотя, учитывая обстановку, складывающуюся на настоящий момент на международной арене, это может довольно скоро измениться. Также следует понимать, что обвинения

противника в ведении информационной войны традиционно являются частью его собственной информационной войны.

В основе большинства концепций информационной войны лежат старые, многократно проверенные методы пропаганды и управления массовым сознанием. На сегодняшний день не только сами эти методы приобретают небывалый размах, но наблюдается и развитие технологий, используемых при ведении информационных войн, и в значительной степени это обусловлено стремительной глобализацией медиапространства.

## 2. Информационные войны в современных международных конфликтах

### 2.1. Борьба государств за цифровой суверенитет в СМИ

В современную эпоху, благодаря развитию технологий и последующему появлению смартфонов и использованию Интернета, социальные сети стали одним из самых популярных источников распространения информации. По оценкам ежегодного исследования Global Digital на 2022 год, 4,6 миллиарда человек, то есть больше половины населения Земли, пользуются социальными сетями. В частности, у Facebook 2,9 миллиарда пользователей, у YouTube — 2,5 миллиарда, а у WhatsApp, принадлежащего Facebook, — 2 миллиарда [19]. Это наиболее часто используемые платформы социальных сетей. Эти форумы являются самым быстрым способом распространения информации, поскольку они позволяют любой информации стать вирусной всего за несколько часов. Кроме того, использование почти всех платформ социальных сетей не требует значительных затрат. Форумы социальных сетей очень удобны и просты в использовании и не требуют какой-либо надлежащей проверки личности лиц, распространяющих информацию. Кроме того, информация, распространяемая через платформы социальных сетей, продолжает достигать всё большей аудитории. То есть информацией можно делиться снова и снова и, таким образом, создается мультипликативный эффект с точки зрения количества людей, которых она может охватить.

Социальные сети - это быстрый способ распространения информации среди большого количества аудиторий и один из наиболее важных инструментов информационной войны. Кроме того, еще одной функцией являются платные кампании на определенных веб-сайтах социальных сетей, таких как Facebook, которые способствуют платному продвижению контента. Эта функция делает общий контент видимым для большего числа пользователей сети. Цена, которую придется заплатить за такие кампании в

социальных сетях, слишком мала. Поскольку кампании позволяют контенту охватить более широкую аудиторию, информационные воины используют его для проведения информационных атак на своих противников. Эти информационные атаки в основном включают в себя распространение дезинформации и пропаганды в социальных сетях против оппонента. Если пропаганда или дезинформация распространяются, чтобы подстрекать или бросать вызов религиозным или идеологическим наклонностям нации, то такая пропаганда может побудить их протестовать против лиц, распространяющих пропаганду в социальных сетях. Повторный обмен контентом может еще больше обострить эмоции и сделать информацию вирусной, охватив большее количество людей и, таким образом, спровоцировав более сильную реакцию. Такое использование социальных сетей может оказаться пагубным для мира, когда они используются антигосударственными субъектами для распространения пропаганды против государств. Здесь социальные сети представляются негативным и смертоносным компонентом информационной войны, поскольку они позволяют любой информации стать вирусной, демонизировать репутацию противника в течение короткого промежутка времени и вызвать бурю негодования и волнений у широкой общественности.

В середине декабря 2010 года в Тунисе началось явление, известное как «Арабская весна». По существу, «Арабская весна» состояла из недовольной молодежи, этнических меньшинств, политических изгоев и научных кругов, участвующих в демонстрациях, протестах и, в конечном счете, революциях. В основном они протестовали против репрессий, цензуры, отсутствия экономических возможностей и нарушений прав человека в правительствах по всей Северной Африке и на Ближнем Востоке. Это движение было подпитано в значительной степени использованием мощи и возможностей мобильных социальных сетей. Кампания почти сразу распространилась вирусно через видео с мобильных телефонов в реальном времени, твиты, хэштеги, Facebook и другие инструменты социальных сетей. Правительства Туниса, Египта, Ливии и Йемена были свергнуты, а многие другие были втянуты в различные волнения

и гражданские войны. Скорость, с которой росла Арабская весна, свидетельствует о мощи мобильных социальных сетей и их повсеместном мгновенном доступе. Границы, океаны и континенты больше не были барьерами для передачи и просмотра живых сообщений из первых рук и средств массовой информации, рассказывающих о быстром росте движения и его эффективности в свержении правительств.

Ранее было установлено, что СМИ рассматриваются как инструмент информационной, и в частности, психологической войны, потому что нарратив среди людей, сформированный СМИ, коренным образом влияет на их психологическое понимание ситуации. В первую очередь именно средства массовой информации формируют мнение людей о каком-либо происшествии или деятельности. Общественное мнение, в свою очередь, играет большую роль в политике с точки зрения принятия решений и легитимности. СМИ также могут разжигать негативные чувства населения, распространяя информацию, ориентированную на ненависть. Например, СМИ могут разжигать патриотические чувства среди людей, распространяя дезинформацию, ориентированную на негативное отношение, о стране-конкуренте. Массы могут начать верить дезинформации, особенно если у большинства людей нет доступа к достоверным фактам об этом конкретном противнике.

Использование средств массовой информации в качестве инструмента информационной войны считается мягким способом ведения информационной войны. Чтобы объяснить это далее, применима «теория фреймов». Фрейм предполагает выбор некоторых аспектов воспринимаемой реальности и модификацию их таким образом, чтобы они стали более заметными в коммуникативном тексте с целью продвижения конкретного определения и восприятия проблемы, причинно-следственной интерпретации, оценки и рекомендации по её решению. В гораздо большей степени, чем в случае с повесткой дня, фрейминг связан с содержанием новостей. Фрейм может быть фразой, изображением, аналогией или метафорой, которую журналист использует для передачи сути проблемы или события. Фреймы упрощают

журналистам процесс написания статей и помогают зрителям понять, с чем они сталкиваются в новостях [20].

То есть средства массовой информации создают для определенного вида деятельности или сущности определенные характеристики и продвигают свои манипулятивные интерпретации этой деятельности. Такое обрамление может либо демонизировать, либо идеализировать эту сущность в зависимости от негативной или позитивной коннотации, приписанной ей средствами массовой информации соответственно.

Часто фреймовая теория становится актуальной при формировании детерминант внешней политики наций, в которой враждебные государства рассматриваются как злые и негативные, а дружественные государства получают положительную репутацию. Это построено с или без использования надлежащей фактической информации. Внешняя политика государства формируется различными факторами, такими как геополитика государства, которые, конечно же, учитываются средствами массовой информации при распространении любого повествования о проблеме. Однако на внешнюю политику и нарративы в СМИ значительное влияние оказывают политическая и экономическая системы внутри государства, его интересы и проблемы. Это видно из эпохи холодной войны, особенно во время правления Рональда Рейгана, когда средства массовой информации США яростно выступали против социалистических и коммунистических планов Советского Союза.

В ту эпоху средства массовой информации США развернули жёсткую информационную кампанию, демонизирующую коммунистические теории. В то же время правительственные учреждения США, особенно Центральное разведывательное управление («ЦРУ»), также поддерживали антисоциалистические нарративы. И СМИ США, и внешняя политика правительства «представляли» Советский Союз и его коммунистическую повестку как угрозу всему миру. На самом деле угроза в то время нависла не над всем миром, а только над капиталистической системой, преобладавшей в Соединенных Штатах в эпоху холодной войны, и, следовательно,

демократическая политическая система Штатов не могла допустить гибели капиталистической системы. Таким образом, для силы и господства своей капиталистической системы в оппозиции к коммунизму и социализму Советского Союза правительство США полагалось на свои средства массовой информации, чтобы начать информационную войну против советского коммунизма. При этом средства массовой информации США полагались на имеющуюся у них информацию, интерпретируемую в соответствии с внешней политикой США в отношении угроз, исходящих от социализма и коммунизма для капиталистической экономической и демократической политической системы Соединенных Штатов. Следовательно, американские средства массовой информации развернули антисоциалистические и антикоммунистические пропагандистские кампании против Советского Союза.

Таким образом, постановка того или иного вопроса внешней политики государства находит своё отражение в информации, распространяемой средствами массовой информации и прочими инновационными коммуникационными технологиями. Кроме того, опираясь на медиа-агентства, государству становится весьма удобно вести информационную войну против противника посредством дезинформации и пропаганды.

Подобное развитие новых технологий, методов и их внедрение в текущую геополитическую и геостратегическую картину мира в сочетании с традиционным пониманием конфликта и безопасности называют «гибридной» войной. Гибридная война представляет собой комбинацию обычной и нетрадиционной войны, выходящей за рамки поля боя и охватывающей экономическую, дипломатическую, информационную и политическую войну. Гибридная война также использует кинетические и некинетические, асимметричные и нетрадиционные средства ведения войны как часть своей гибридной стратегии [21]. В связи с этим гибридная война также использует информацию как оружие против своего противника. В таком сценарии информация используется в виде пропаганды, дезинформации, фейковых новостей. Все эти действия также являются тактикой информационной войны,

что создаёт наложение стратегий между гибридной войной и информационной войной. Поскольку гибридная война представляет собой более широкий спектр стратегий, включающих тактику информационной войны, можно утверждать, что последняя является элементом гибридной войны. Когда определённые действия, такие как пропаганда, ведутся через новости или социальные сети против противника, и распространяются так, что создают у аудитории убедительный негативный образ врага, репутация последнего оказывается запятнана, в результате чего он теряет поддержку со стороны международного сообщества. Когда в вооруженном конфликте используются другие тактики информационной войны, как DDoS-атаки и взлом, то противник также оказывается в невыгодном конкурентном положении, и в силу скрытного характера действия информационные операции по типу DDoS-атак являются элементом гибридной войны. Таким образом, информационная война произвела революцию в аспектах обычной войны, превратив Интернет и киберпространство в зону боевых действий, заменив обычные поля сражений. Киберпространство стало новым полем боя, где информационные воины могут, не проливая крови, нанести существенный нематериальный ущерб, разрушив репутацию оппонента, похитив его стратегически важные данные или сделав его системы безопасности уязвимыми для атак. Государства и негосударственные субъекты теперь ведут гибридную войну, полагаясь только на тактику информационной войны и используя информацию в качестве оружия против своих противников. Тем самым информационная война упростила гибридную войну.

Со временем весь земной шар начал ощущать влияние социальных сетей и других медиа как инструмента информационной войны. Операцию «Буря в пустыне» в Ираке Соединённых Штатов и их союзников по коалиции 1991 года, часто называют «первой информационной войной». В ходе операции был создан информационный дифференциал, парализовавший системы противника. Авиация коалиции нанесла удары по радиостанциям, телефонным станциям и микроволновым станциям. Совместно с дивизионами по радиоэлектронной

борьбе велась радиопропаганда, следовательно, оказывалось воздействие двух опаснейших методов информационной войны - физических атак и атак на данные. Эта операция подпитала ожидания военных и политических сил множества государств, стремящихся доминировать в информационном спектре. История информационных войн насчитывает немало других примеров: «революция роз» в Грузии в 2003 году; «оранжевая революция» в Украине 2004 года; попытка «джинсовой» революции в Беларуси 2006 года; российско-грузинская война в 2008 году, а также украинский «Евромайдан» 2013 - 2014 гг. [22].

С распространением Интернета, в 90-е гг. военные и политические элиты Америки начали использовать термин «информационная война» в своих документах, а механизмы информационных операций начали постепенно внедряться в военную и внешнеполитическую доктрины Соединённых Штатов. Инструменты умной и мягкой силы, сопряжённые с вопросами информационной политики, также находят отражение в национальных интересах Америки, поэтому влияние технологий манипулирования сознанием через СМИ быстро нашло применение во внешнеполитической деятельности Соединённых Штатов [23]. Мощности своей информационной деятельности США неоднократно направляли на Российскую Федерацию, создавая в лице России образ всеобщей мировой угрозы, и сейчас эта конфронтация нарастает на всех направлениях – от Латинской Америки до Донбасса.

Конфликт в информационном пространстве между двумя державами начался задолго до событий, о которых пойдёт речь далее, однако новый виток информационная война как явление и, в частности, элемент международных отношений 21 века, получила именно в 2022 году, когда главным полигоном информационной войны стала Украина. 21 февраля 2022 года президент Российской Федерации Владимир Владимирович Путин обратился к россиянам после обсуждения вопроса о признании Россией Донецкой и Луганской народных республик. Президентом были подписаны соответствующие указы, а также договоры о дружбе, сотрудничестве и взаимной помощи с этими

республиками. Главы ДНР и ЛНР — Денис Пушилин и Леонид Пасечник — обратились к Владимиру Владимировичу с просьбой оказать помощь в отражении агрессии со стороны Вооруженных сил Украины во избежание жертв среди мирного населения и предотвращения гуманитарной катастрофы. 24 февраля 2022 года Президент РФ обратился к гражданам с сообщением, что принял решение о проведении военной спецоперации на Донбассе. Целью данной операции является защита людей Донбасса, которые подвергались издевательствам и геноциду со стороны Киева, в связи с чем Россия стремится к денацификации и демилитаризации Украины. Подчёркивалось, что речи об оккупации государства не идёт. В. Путин также заявил, что силы, совершившие на Украине госпереворот, захватили власть и отказываются от мирного урегулирования конфликта на Донбассе. Восемь лет Россия делала всё возможное, чтобы решить ситуацию мирными средствами, но усилия ничем не обернулись. По словам президента, у Российской Федерации не оставалось иного выхода для защиты страны и народа, кроме того, которым Москва была вынуждена воспользоваться, поскольку обстоятельства требовали незамедлительной реакции.

Практически сразу после обращения главы РФ агентство ТАСС сообщило о взрывах возле аэропорта Борисполь под Киевом [24]. Эту информацию подтвердили в Минобороны России, сообщив также об ударах по украинским военным аэродромам. Как уточнялось ведомством, высокоточным оружием выведены из строя военная инфраструктура, объекты ПВО, военные аэродромы и военная авиация Украины. Однако никаких ракетно-авиационных или артиллерийских ударов по украинским городам российские силы не наносят, точечные удары по военной инфраструктуре происходят без угрозы гражданскому населению [25].

С началом спецоперации в сети начали появляться расследования, проливающие свет на пропагандистские методы и раскрывающие новые факты создания фейков. Если ранее кампании информационной войны были более «закулисными», то сейчас Запад даже не скрывает собственных действий. Так,

компания Meta разрешила в своих соцсетях публиковать в открытый доступ призывы к насилию в отношении россиян. В посольстве РФ в США назвали действия Meta объявлением информационной войны без правил [26], а украинский лидер Владимир Зеленский поблагодарил руководство Meta за их вклад в информационную войну [27]. В ответ российские власти заблокировали социальные сети Meta, чтобы оградить людей от откровенно деструктивной провокационной информации.

Говоря о методах пропаганды, то они разнообразны. Например, выяснилось, что в Telegram созданы группы, где украинские провокаторы координируют информационные атаки на россиян, в частности, на матерей российских военнослужащих.

Очевидно, что западные СМИ скрывают информацию о реальных негативных действиях Запада и Украины. Проанализировав ряд иностранных СМИ и официальных документов мы обнаружили, что везде власти США отрицают свою причастность к работам биолабораторий на Украине и к ракетному удару, нанесённому по Донецку.

Так, например, итальянская газета La Stampa разместила фотоснимок, сделанный в Донецке после обстрела ВСУ и преподнесла это как последствия обстрела Киева [28]. Официальный представитель МИДа РФ Мария Захарова назвала данную публикацию примером особого цинизма. В своём Telegram-канале дипломат пишет: «Спасатели, тела, люди в горе, следы разрушений. Всё это — последствия обстрела, совершенного ВСУ в ДНР при помощи тактического ракетного комплекса «Точка-У»... Будто это в Киеве лежат тела жертв боевых действий, а не в Донецке. Этот фейк показателен… Всё сгодится ради шокирующей подачи информации в антироссийском угаре. И никому нет дела до правды. Все обслуживают одну сторону баррикад» [28]. Стоит отметить, что на критику и негодование со стороны итальянских читателей газета отреагировала, заблокировав функцию обратной связи на своём сайте.

Активно распространяются и другие фейковые сообщения. Например, распространялась информация о том, что в ходе боёв за Мариуполь, 9 марта в

результате обстрела или авиаудара якобы пострадала городская больница №3. Информационное агентство Associated Press опубликовало фотографии украинского внештатного фотожурналиста из родильного дома, на нескольких из которых запечатлена беременная женщина с лёгкими травмами. Впоследствии оказалось, что это постановочная фотосъёмка с известной в регионе инстаграм-моделью и бьюти-блогером Марианной Подгурской, а сам роддом давно не действует, в нём засели боевики «Азова» [29]. На видеосъёмке с места действия не видно остальных «жертв» атаки, а в ходе расследования, предоставленного порталом «войнасфейками.рф.» выяснилось, что съёмка велась не в роддоме, а в офтальмологическом отделении, прекратившем работу через несколько дней после начала спецоперации, следовательно, ни пациентов, ни обслуживающего персонала там быть не могло, не говоря уже о том, что «Азов» и другие радикалы выгнали оттуда и рожениц, и персонал при захвате, сделав из здания базу [30]. Постоянный представитель Российской Федерации при ООН Василий Небензя в Совбезе ООН продемонстрировал фотографии, разоблачающие фейк и высказался следующим образом: « - … эта блогерша на двух фотографиях загримирована как две разные женщины. Нас возмущает гнусная, грязная кампания по очернению российских военных, которая обвиняет их в преднамеренных атаках на гражданские объекты» [31].

На этом ложные сообщения о действиях в Мариуполе не прекратились. 16 марта украинские власти, а позже и ряд западных СМИ заявили, что ВКС России нанесли бомбовый авиаудар по Мариупольскому драматическому театру и бассейну «Нептун». После атаки украинские власти сообщили, что оба объекта использовались в качестве бомбоубежищ для мирных жителей, в том числе беременных женщин и детей, и назвали бомбардировку военным преступлением. Минобороны РФ отреагировало, отметив, что здание театра никогда не считалось объектом для поражения. ВКС России вообще не наносили авиаударов по наземным объектам в городе Мариуполь. В ведомстве подчеркнули, что «Азов» ранее заминировал здание и разместил на его верхних

этажах «огневые точки», а 16 марта взорвал театр, таким образом осуществив «кровавую провокацию» [29].

Особенно изощрённым случаем дегуманизации и дискредитации российских военнослужащих в глазах мирового сообщества в рамках военной спецоперации стали события в украинском городе Буча в Киевской области. 3 апреля Украина и ряд стран Запада обвинили Россию в преступлении против человечности – массовом убийстве мирных граждан. Как доказательства приводились спутниковые снимки и журналистские свидетельства. Официальные представители РФ назвали произошедшее провокацией. Пресс-секретарь президента Российской Федерации Дмитрий Песков призвал лидеров западных стран и членов Совета Безопасности обратить внимание на очевидный и жестокий подлог с целью очернить российскую армию и признал возможность появления новых фальсификаций. В Минобороны подчеркнули, что российские военные не блокировали выезды из города и полностью покинули Бучу за четыре дня до появления демонстрируемых свидетельств, когда в город прибыли Службы безопасности Украины [29]. Также Минобороны были приведены обстоятельные доказательства сфабрикованности спутниковых фото и видео с места действия от украинских и западных СМИ. Известный российский журналист Андрей Медведев высказался о том, что провокация произошла именно в городе Буча в связи с созвучностью этого слова с английским “butcher”, что в переводе означает “мясник” - игра слов западных медиа для усиления эмоционального эффекта. Также журналист подчёркивает, что данную информационную войну необходимо вести с учётом западного восприятия россиян и отношения к России, внедряя тактики и стратегии как и при обычных боевых действиях, но другими средствами [32]. Принимая во внимание ознаменовавшие новый виток противостояния Запада и Российской Федерации высылку российских послов из ряда стран, очередной пакет санкций, наращивание военной и финансовой поддержки киевского режима и визиты в Украину европейских политических деятелей, небезосновательны в этой связи высказывания министра

иностранных дел РФ Сергея Лаврова о том, что появление сообщений о «резне» в Буче является попыткой сорвать переговоры между Россией и Украиной [29]. Провокация в Буче имеет особую международную и символическую значимость. Для России такая мощная попытка дискредитации знаменует собой новый этап давления и персонифицированную атаку на политическое и военное руководство страны.

Василий Небензя заявил, что в сети размещено уже более миллиона фейковых сообщений, порочащих военную спецоперацию на Украине [33]. Их распространению способствует даже такая интернет-площадка как «Википедия», предусматривающая редактирование и создание информационных статей для всех желающих. Интернет-хулиганы переиначивают факты, называя «войной» и «оккупацией» спецоперацию, создают новые разделы, извращающие действия Российской Федерации.

Обвинения России в военных преступлениях схожими методами и даже эксплуатирование схожих тем происходили в рамках информационной войны, проходившей в 2015 и 2016 гг. параллельно с войной в Сирии.

Сирийский центр мониторинга за соблюдением прав человека 1 октября 2015 года, ссылаясь на источники в сирийской оппозиции, обвинил российских лётчиков в уничтожении госпиталя в провинции Хама. Бездоказательный вброс о бомбардировках невоенных объектов подхватили западные СМИ и правозащитники, и продолжилась данная линия в ноябре того же года обвинениями Минобороны РФ в авиаударе по больнице в Сармине [34]. При помощи аэрофотосъёмки российское военное ведомство доказало, что здание было разрушено ещё до вмешательства российских войск в сирийский конфликт. Международная организация Amnesty International в декабре 2015 года опубликовала доклад, где вновь Россия бездоказательно обвинялась в намеренном проведении серии авиаударов по медицинским учреждениям и школам Идлиба, Хомса и Алеппо, что было опровергнуто Минобороны России.

Информационная война против действий России в Сирии с новой силой развернулась в 2016 году, достигнув пика, когда Сирийская Арабская армия

(«САА») при поддержке ВКС России начали брать в кольцо Алеппо [34]. Чем ближе войска подходили к городу, тем чаще стали появляться сообщения об уничтоженных больницах и школах, а также вброс о ракетном ударе по мечети в деревне Аль-Джуна. Правозащитники ссылались на данные волонтёров из якобы гуманитарной организации «Белые каски», которые неоднократно уличались в создании постановочных видео [35].

Детская тема в рамках информационной войны в Сирии также активно эксплуатировалась. В сентябре 2016 года стала известна история семилетней девочки Бана Алабед, которая якобы активно вела свой блог в сети Twitter, где делилась подробностями тяжёлой жизни в осаде, призывая мировое сообщество оказать давление на президента Сирии Башара Асада и российское руководство. При этом сообщения, написанные слишком хорошим и грамотным английским языком для семилетнего ребёнка, поступали из района, отключенного от Интернета и электричества. Показателен также случай пятилетнего мальчика Омрана – западного символа Алеппо. Видео, где окровавленного мальчика в пыли спасают из-под завалов, стало вирусным во всём мире. Правозащитники вновь обвинили российскую авиацию – якобы на них лежит вина за уничтожение дома ребёнка. Впоследствии был доказан постановочный характер видеофайла [35].

Это лишь одни из множества примеров постановочных информационных кампаний со стороны Запада. Однако в то время как Запад отвергает российские взгляды, некоторые влиятельные акторы в развивающихся странах и в Китае слушают и принимают их. Даже ряд теоретиков в США поддерживает Россию, однако неизменно такие люди считаются «сторонниками теории заговора» со стороны официального правительства Америки. Китай, который более жёстко контролирует свой Интернет, чем любая другая страна в мире, продвигает позицию Москвы. Китай и Россия решили укрепить свое сотрудничество в области СМИ в 2015 году, и текущая информационная война показала успех этой инициативы. Через несколько часов после начала спецоперации 24 февраля газета Коммунистической партии

Китая Global Times опубликовала видеозапись, что большое количество украинских солдат сдалось в плен, со ссылкой на российскую государственную медиасеть RT. Затем китайская государственная центральная телевизионная станция (CCTV) сообщила и распространила в социальных сетях, что Зеленский бежал из Киева. Китайские СМИ повторили позиции России о том, что военная спецоперация противостоит Западу, расширению НАТО, нацизму и фашизму и поэтому оправдана. Сообщалось, что Украина использует мирных жителей в качестве живого щита и пытает пленных солдат.

Возможно, самым опасным для США было то, что китайские правительственные чиновники распространили заявления России о том, что Пентагон финансирует биологическое оружие на Украине. Китайские правительственные чиновники обратили на это внимание на пресс-конференциях, в прессе и в официальных аккаунтах в социальных сетях - на китайском, арабском и английском языках. Это заявление в информационных источниках США также считается «теорией заговора». Поддержка России рядом африканских стран также представляет для США и её союзников по НАТО угрозу, так как они стремятся развивать более прочные отношения с богатыми ресурсами африканскими государствами в немалой степени для того, чтобы снизить ресурсную зависимость от России и Китая. В этой связи западные страны могут обнаружить, что им не доверяют как политическим и деловым партнерам. Российская позиция может также нанести ущерб долгому стремлению США к расширению сотрудничества в области безопасности с Индией. Китай со своей стороны имеет явные преимущества от поддержки российской позиции. Поскольку западные бизнес-корпорации массово покидают Россию, Китай является государством, наиболее полно способным внедриться в освободившиеся рыночные экономические позиции. США уже давно опасаются укрепления российско-китайского партнерства, и текущая информационная война в сочетании с экономической войной стали катализатором для подобных опасений.

Стратегии информационной войны Китая как одного из влиятельнейших международных акторов стоит уделить отдельное внимание. Китайская стратегия информационной войны фокусируется на использовании создания и поддержания информационного превосходства. Операции в киберпространстве используются для достижения информационного господства посредством разведки и шпионажа, проведения сетевых вторжений. Китайская концепция «неограниченной войны» сочетает в себе элементы информационных операций, операций в киберпространстве, нерегулярных боевых действий, проводимых как в мирное время, так и в условиях конфликта. Соединенные Штаты рассматриваются как противник, чьи преимущества можно преодолеть с помощью стратегии информационных операций. Зависимость США от технологий, как в вооруженных силах, так и среди гражданского населения, создаёт уязвимость, которую можно использовать, наряду с «теоретическими слепыми зонами» и «ошибками мышления», такими как отсутствие всеобъемлющей теории в доктрине Министерства обороны США, которая сочетает в себе все элементы информационной войны. В киберпространстве шпионаж за компьютерными сетями играет большую роль в усилиях Китая по достижению конкурентного преимущества. В 2009 году Китай подозревался в краже больших терабайт данных о конструкции истребителя F-35 Joint Strike Fighter с компьютеров оборонного подрядчика Lockheed Martin. В 2014 году гражданину Китая было предъявлено обвинение в краже конфиденциальных коммерческих секретов оборонных подрядчиков, в частности данных, касающихся военно-транспортного самолета Boeing C-17 [36]. Промышленный шпионаж, подобный этому, приносит экономические выгоды, а также преимущества в военной сфере и национальной безопасности для Китая, подрывая при этом техническое превосходство Соединенных Штатов.

Что касается обороны, то Китай использует сочетание правовой политики и информационных технологий для цензуры в рамках программы под названием «Золотой щит». Её часто называют «Великим китайским брандмауэром». Кроме того, Китайская Народная Республика активно

продвигает идею «киберсуверенитета», устанавливая границы в Интернете на основе территориальной целостности. Китай также вложил значительные средства в киноиндустрию, чтобы получить культурное и экономическое влияние, хотя постепенно отношения Китая с Голливудом начали остывать. Китай также представляет образ себя как мирной нации, сосредоточенной на внутреннем развитии, а не на стремлении к международной власти. Китайская доктрина информационной войны предполагает, что эта тактика является частью более широкой стратегии поощрения самоуспокоенности потенциальных противников. Другая тактика включает использование международных форумов для продвижения идеи контроля над вооружениями для «информационного оружия», чтобы сохранить контроль над собственным информационным аппаратом и уравнять правила игры с технологически развитыми державами [36].

Резюмируя, стоит вновь подчеркнуть, что на сегодняшний день информационная война в целом и, в частности против Российской Федерации, планируется в некотором смысле тщательнее военных действий. Очевидно, что основная цель информационных операций - посеять недоверие к армии, власти, привести к перевороту и упразднению суверенного развития страны. В игру вступает всё больше государств, а военная спецоперация на Украине ещё идёт. Появление новых провокаций – это лишь вопрос времени. Сегодня медиа-пространство во взаимосвязи с информационными войнами характеризуется увеличением объёма и скорости передаваемых и добываемых новых информационных сообщений, их обработки и использования, а также усилением технической оснащённости.

## 2.2. Нормы международного права в сфере информационного противоборства.

Некоторые из норм международного права, например, Договор о космосе 1967 года — в конечном итоге косвенно облегчают условия, поддерживающие

продолжение информационной войны, оставляя цифровую сферу неконтролируемой в контексте соответствия с международным правом [37]. С другой стороны, сложная и разносторонняя арена информационной войны затрудняет регулирование и контроль информационных операций с помощью международных норм и принципов. Например, право вооруженных конфликтов и международное гуманитарное право пытаются регулировать поведение субъектов, участвующих в информационной войне, однако неосязаемость ущерба, причиняемого информационной войной, затрудняет введение ограничений.

Право войны или право вооруженного конфликта защищает гражданских лиц и некомбатантов в вооруженном конфликте. Точно так же право войны пытается защитить гражданских лиц от любого информационного нападения. То есть стороны, ведущие информационную войну не должны причинять вреда гражданскому населению. Это правило может применяться к деятельности по взлому или нарушению любой технологической передачи враждебного государства путем ведения информационной войны. Если такая деятельность каким-либо образом наносит ущерб гражданскому населению – например, в нарушении их бизнеса, повседневной жизни и т.д. — тогда такая деятельность должна считаться незаконной в соответствии с международным гуманитарным правом или правом войны [38].

На самом деле существует ещё множество проблем, с которыми сталкивается международное право, в частности международное гуманитарное право или право войны, при регулировании информационной войны. К сожалению, из-за таких вызовов международное право становится парализованным в попытке регулировать или контролировать обширную и сложную область информационной войны и информационные операции, предпринятые юридическим лицом против своего противника. Международное право, в частности международное право вооруженных конфликтов, ничего не говорит о нематериальном ущербе, причинённом противнику во время войны и мира.

То, что именно входит в термин «нематериальный ущерб», зависит от режима информационной операции, направленной против противника; например, когда средства массовой информации используются для ведения пропаганды или когда социальные сети используются для клеветы, неосязаемость заключается в подрыве репутации противника. С другой стороны, когда дезинформация используется в качестве оружия информационной войны, она неосязаема с точки зрения лишения людей достоверной информации и фактов об определенной деятельности в военное или мирное время. Во всех этих случаях ущерб не является физическим или материальным, что в конечном счёте исключает принципы международного права как неприменимые к таким ситуациям. Следовательно, становится невозможным регулировать такую деятельность по информационной войне. Однако существуют определенные исключения, когда нематериальный ущерб также приводит к материальному ущербу. Например, при вторжении в киберпространство противника путем внедрения вредоносного ПО или вируса в стратегически важные программные системы противника нематериальный ущерб может привести к ощутимым потерям в виде повреждения инфраструктуры или человеческих жизней. Например, взлом реактивных истребителей противника или атака на них с помощью вредоносных программ могут привести к колоссальным финансовым потерям, а также к человеческим жертвам. Однако международное право не дает достаточных указаний в отношении такого поведения государств во время войны. Как видно из вышесказанного, в международном праве существуют значительные пробелы в регулировании деятельности информационных войн.

Отдельно стоит затронуть неотъемлемое право на свободу мнений и их свободное выражение. Когда борцы за информацию используют средства массовой информации или социальные сети для ведения пропаганды или распространения дезинформации среди населения, тогда право человека на свободу мнения и его свободное выражение становится актуальным в предоставлении свободы борцам за информацию в использовании СМИ или

социальных сетей для распространения нарративов, которые они создают против своего противника. Право на свободу мнений и их свободное выражение защищено Всеобщей декларацией прав человека (ВДПЧ), принятой Организацией Объединенных Наций в 1948 году. Текст статьи 19 Всеобщей декларации прав человека подтверждает это право следующими словами: «Каждый человек имеет право на свободу мнений и их свободное выражение; это право включает свободу беспрепятственно придерживаться своих мнений и свободу искать, получать и распространять информацию и идеи любыми средствами независимо от государственных границ» [39]. «Свобода беспрепятственно придерживаться своих мнений», таким образом, ставит перед международным правом задачу ограничить любое мнение или выражение, выраженное в статье. Именно международное обычное право способствует реализации права на свободу мнений и их свободное выражение. Единственное, что может помешать использовать своё право на свободу мнений и их свободное выражение для ведения информационной войны, — это юридические доказательства противником диффамационного характера их выражения мнений путем подачи исков против них в суд в соответствии с международно-правовыми протоколами. Таким образом, борцы за информацию могут быть юридически ограничены в выражении своего мнения, если в суде будет доказано, что такие мнения являются преступлением на почве ненависти или полностью диффамационными. В противном случае неотъемлемое право на свободу мнений и их свободное выражение используется информационными борцами не по назначению в качестве оружия. Следовательно, взаимосвязь между тактикой информационной войны и правом на свободу мнений и их свободное выражение в соответствии со статьей 19 ВДПЧ становится сложной задачей для международного права. Это приводит к постоянному продолжению информационных операций государств и негосударственных субъектов против своих противников.

Возвращаясь к договору о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и

другие небесные тела, который также известен как Договор по космосу, официально ратифицированному в октябре 1967 года, стоит отметить, что согласно этому договору космос и все небесные объекты являются общим достоянием всего человечества. Аналогичный принцип представлен в Лунном договоре, утвержденном в 1979 г. Согласно Лунному договору, Луна и все её ресурсы являются общим достоянием всего человечества. Следовательно, из этих двух договоров можно утверждать, что комическое пространство и ресурсы его небесных объектов, включая Луну, могут использоваться бесплатно [37]. Это утверждение было дано в соответствии с принципом общего наследия человечества, который гласит, что любой объект или собственность, являющиеся общими для всего человечества, должны быть свободны для использования всеми странами. Данный принцип наряду с Договором о космосе применим к информационной войне, потому что большинство информационных операций осуществляется посредством передачи радиоволн, которые распространяются в пространстве [40]. То есть, будь то передача новостей по радио или телеканалу, распространение информации через платформы социальных сетей или вторжение в киберпространство путём взлома через Интернет, используются радиоволны, передаваемые с искусственных спутников, отправленных в космос с помощью крупных международных телекоммуникационных агентств или правительств. Следовательно, всякий раз, когда имеет место какое-либо из вышеупомянутых действий информационной войны, космическое пространство становится средой передачи радиоволн и, следовательно, облегчает пути информационных операций. Вместе с тем, поскольку в соответствии с Договором о космосе и принципом общего наследия человечества космос является общим достоянием всего человечества и может свободно использоваться всем человечеством, использование космоса является бесплатным для всех, даже для ведения операций информационной войны. Таким образом, косвенно Договор по космосу и принцип общего наследия человечества обеспечивают правовую защиту для продолжения операций информационной войны.

Следовательно, международное право имеет жёсткие ограничительные рамки в регулировании сферы информационного противоборства. Ограничения в основном связаны с нематериальностью ущерба, причиняемого информационной войной. Кроме того, международная защита неотъемлемого права на свободу мнений и их свободное выражение, закрепленного в статье 19 ВДПЧ, ещё больше закрепляет неспособность международного права регулировать определенные информационные операции, такие как ведение пропаганды против противника через средства массовой информации или социальные сети. Также, Договор о космосе и принцип общего наследия человечества допускают распространение информации с помощью радиоволн, передаваемых с искусственных спутников, отправленных в космос, даже если такая информация развёртывается или используется информационными воинами в их соответствующих информационных операциях. Таким образом, косвенно или непреднамеренно международное право способствует информационным операциям, а не регулирует или контролирует их. Поэтому для международных юристов стало проблематично разрабатывать способы контроля и регулирования информационных операций.

8 марта 2022 года Региональный общественный центр интернет-технологий (РОЦИТ) выдвинул в ООН предложение инициировать создание так называемых норм о цифровом нейтралитете в период вооруженных конфликтов с целью детерменирования и регламентации различных аспектов информационного освещения таких конфликтов. Подобная инициатива стала бы важным шагом на пути к укреплению и стабилизации мирового сообщества в условиях глобальной цифровизации и развития новых технологий [41].

Международному сообществу действительно необходимо решить и оценить правовые проблемы в области регулирования информационной войны, чтобы контролировать угрожающий рост информационных операций со стороны государств и негосударственных субъектов, ведущих информационную войну или же гибридную войну против своих противников. Одно из наших предложений по регулированию информационной войны для

приведения её в соответствие с юридическими нормами международного права состоит в том, чтобы принять новые законы, правила и принципы, а также разработать новую конвенцию, которая не только регулировала бы информационную войну, но и устраняла проблемы, вызванные другими договорами и принципами международного права в контроле над ареной информационной войны.

В настоящее время не существует конкретного набора правил или политик в рамках международного права, которые могли бы определять или регулировать информационные операции. Правовой вакуум в этом отношении огромен, и его необходимо заполнить, чтобы воспрепятствовать вредоносному применению информационных войн. Этот вакуум можно заполнить, если под эгидой международного права будут разработаны новые правила и принципы, регулирующие поведение сторон, участвующих в информационной войне. Соответствующее сотрудничество международного сообщества может оказаться полезным в этом отношении, поскольку некоторые государства, например европейские и скандинавские государства, могут поделиться своим успешным опытом сдерживания разжигания ненависти, дезинформации и пропаганды на своих внутренних аренах. Здесь государства также должны сотрудничать друг с другом для обсуждения различных аспектов, инструментов и областей, в отношении которых требуется особый правовой контроль для регулирования сложной сферы информационной войны. Например, использование СМИ для распространения ложной информации является активной площадкой для ставок информационной войны против своих противников. Следовательно, эта платформа должна быть проанализирована, а затем тщательно отрегулирована таким образом, чтобы не только защитить необходимую свободу мнений и их выражения, но и контролировать любую негативную, деструктивную деятельность, осуществляемую через СМИ в сфере информационной войны. Предлагается сформулировать на международном уровне специальный кодекс поведения, разработанный для международных информационных агентств, для предотвращения криминализации

распространения пропаганды и разжигания ненависти. Новые положения должны предусматривать пресечение негативной пропаганды против государств, религий, рас, этнических сообществ и т.д. Будет ли такая политика осуществляться напористо или нормативно — это ещё один вопрос, который необходимо решить, и который международное сообщество должно вынести на повестку дня после оценки ситуации. преимуществ и недостатков каждой стратегии. Тем не менее, правила и принципы, направленные на пресечение фальшивых новостей, разжигания ненависти и пропаганды, могут быть реализованы в нормативном смысле, но их нормативность может сделать их устойчивыми в будущем лишь в случае, если всё международное сообщество и Организация Объединенных Наций в конечном итоге поддержат их положительно. Таким же образом можно решать и регулировать все остальные аспекты информационной войны.

На сегодняшний день также не существует ни единой конвенции по вопросу регулирования информационных войн, в то время как государства и негосударственные субъекты стали всё более интенсивно использовать тактику информационной войны против своих соперников, что представляет серьезную угрозу международному миру и безопасности. В частности, когда террористы распространяют определённую информацию — например, Талибан извлекал выгоду из использования информационной войны наряду со своей стратегией законности против сил НАТО в Афганистане, — это, следовательно, подрывает эффективность операций против них. Хотя призывы по разработке новой международной политики для регулирования растущих механизмов информационной войны в современную эпоху пока не набрали достаточных оборотов, рациональность и практичность, стоящие за ними, весьма убедительны, и мир должен серьезно задуматься над этим. Если призывы к разработке новой конвенции по регулированию информационной войны будут услышаны и восприняты положительно и будет принята новая конвенция, то она безусловно станет новой «площадкой» для анализа и регулирования различных областей информационной войны. В частности, она станет

специальной площадкой для государств, юристов и органов международного права для обсуждения различных аспектов информационной войны и выслушивания предложений по совместной разработке нового кодекса поведения или правил для регулирования информационных операций. Кроме того, это также закроет существующие лазейки и дыры в международном праве, которые косвенно облегчают проведение операций информационной войны. Необходима рамочная основа для содействия расстановке приоритетов и планированию, а также для представления целей, которые могут быть достигнуты с помощью информационной войны. Планировщики должны четко сформулировать, почему предпринимается конкретное действие и когда оно должно произойти, основываясь на намерениях командира, оперативной обстановке и оперативном подходе, разработанном для решения проблемы. Именно сейчас настало время подчинить информационную войну международно-правовым нормам и принципам, поскольку это поможет смягчить будущие угрозы, создаваемые для международного мира и безопасности.

# ЗАКЛЮЧЕНИЕ

В современную эпоху технического прогресса информационные войны активно разворачиваются государствами и негосударственными субъектами против своих противников. Информационная война влечёт за собой распространение манипулируемой информации или доступ к определённым данным, а затем использование этой информации для получения конкурентного преимущества. Некоторые примеры информационной войны включают распространение пропаганды или дезинформации с использованием средств массовой информации, распространение вредоносных программ или вирусов в компьютеризированные системы военного управления или другие стратегически важные учреждения, кражу важных данных путем взлома и демонизацию противника посредством использования электронных средств массовой информации или платформ социальных сетей.

Все эти тактики информационной войны меняют состояние войны в нынешнюю эпоху. Война теперь ведётся на новых технологических фронтах, потому что государства и прочие институты осознали важность укрепления систем безопасности своих стратегически важных наборов данных и компьютерных систем. С этой целью госучреждения внедряют специальные меры безопасности для предотвращения угроз информационной войны. Определенная тактика информационной войны может оказаться смертельно опасной для международного мира и безопасности; например, дезинформация и пропаганда — это тактика, которая может усугубить напряженность между противоборствующими государствами и привести к конфликту, если государства будут вовлечены в непрекращающиеся пропагандистские войны друг против друга. Пропаганда — мощный инструмент, и, как было доказано, при эффективном использовании она способна манипулировать населением в огромных масштабах. Использование социальных сетей для управления тенденции делает распространение пропаганды легче, чем когда-либо прежде для как государственных, так и негосударственных субъектов.

Ситуация может стать критической, если террористы овладеют хакерской стратегией и смогут распространять вредоносное ПО или вирусы или дистанционно контролировать стратегически важные компьютерные системы государства-противника. В таком случае угроза региональному миру и ущерб репутации безопасности государства могут быть массовыми. Поэтому настало время упорядочить тактику информационной войны, пока не стало слишком поздно. Тем не менее, несмотря на вышеупомянутые угрозы международному миру и безопасности, на международном уровне, к сожалению, не было разработано механизма, политики или свода правил, которые могли бы регулировать сферу информационной войны. Более того, до сих пор нет ни одной конвенции под широкой эгидой международного права, в которой обсуждалась бы необходимость регулирования или контроля информационных войн. Тенденция последних нескольких десятилетий заключается в том, что международное сообщество не принимает во внимание призывы к разработке отдельной конвенции по какому-либо вопросу, если только этот конкретный вопрос не станет глобальным и очень важным по своему характеру. Таким образом, до сих пор не было предпринято усилий по разработке ни отдельной конвенции, ни специальных правил, которые могли бы услышать призывы к регулированию информационных войн.

Прогнозы катастрофической кибератаки доминировали в политических дискуссиях, но мало кто осознавал, что социальные сети могут быть использованы в качестве оружия против сознания населения. Случаи США и Украины — модели этой будущей войны, в которой социальные сети используются для прямого влияния на людей. По мере совершенствования технологий, усовершенствования методов и распространения интернета по всему миру станет действовать закон: тот, кто контролирует тенденцию, будет контролировать повествование, и, в конечном счете, повествование управляет волей людей.

Чтобы сформировать среду, соответствующую желаемым состояниям, мы должны признать важность информационной войны и работать над тем, чтобы

концепции ввода-вывода были интегрированы во все действия и операции. Наши специалисты по информационным операциям должны иметь подготовку и опыт, необходимые для удовлетворения этих требований в качестве стратегического руководства. Если мы не сможем достичь этих целей, то будем отставать в постоянно меняющемся мире информационных технологий и будем неэффективны. Пришло время форсировать изменения через устойчивый и воспроизводимый процесс и организацию.

По мере того как мир продолжает вступать в информационную эпоху, способность национальных государств и негосударственных субъектов использовать успешные тактики информационной войны в своей общей стратегии, несомненно, возрастёт. Чтобы успешно сдерживать эти угрозы и реагировать на них, Российская Федерация должна внедрять инновации и развивать организации, обладающие опытом как в предотвращении, так и в проведении таких действий. Определение понятийного аппарата, разработка оперативных концепций информационной войны и смена ресурсов позволят нашим силам сражаться и побеждать в информационную эпоху. Настала пора активнее переходить в информационную контратаку, создав новую структуру, ответственную за развитие информационных мощностей и управление ресурсами – например, российскую расследовательную комиссию по делам по типу украинской Бучи, чтобы иметь возможность перехвата новостной повестки мощными информационными залпами, подкреплёнными доказательной базой, в качестве ответа Западу. Работа с молодёжной аудиторией также имеет особую важность для отстаивания национальных интересов внутри государства.

По мере продвижения вперёд в информационную эпоху наша жизнь будет всё больше переплетаться и связываться с информационными системами. Эта информационная среда будет продолжать играть решающую роль в том, как правительство и военные взаимодействуют с союзниками и противниками во всех оперативных областях.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Merriam-Webster's collegiate dictionary // Merriam Webster's Collegiate. – Springfield, MA, 2004. – ISBN 978-0-87779-807-1. – P. 555-556.

2. Merriam-Webster's collegiate dictionary // Merriam Webster's Collegiate. – Springfield, MA, 2004. – ISBN 978-0-87779-807-1. – P. 358-359.

3. Сунь-Цзы, Искусство войны и искусство управления : перевод военного трактата / Сунь-Цзы, Г. Галиарди. – Санкт-Петербург : Нева, 2003. – 160 с. – ISBN 5-7654-2459-7.

4. Барабаш, В. В. Информационные войны и медийное пространство: теоретические аспекты новейших изменений / В. В. Барабаш, Е. А. Котеленец // Известия высших учебных заведений. Поволжский регион. Гуманитарные науки. – 2016. – №. 3 (39). – С. 150-158.

5. Britannica Dictionary definition of propaganda // Britannica : официальный сайт. – URL: https://www.britannica.com/dictionary/propaganda (дата обращения: 02.05.2022).

6. Барабаш, В. В. Информационная война: к генезису термина / В. В. Барабаш, Е. А. Котеленец, М. Ю. Лаврентьева // Знак: проблемное поле медиаобразования. – 2019. – №. 3 (33). – С. 76-89.

7. Longley, R. An Introduction to Psychological Warfare / R. Longley // ThoughtCo : [сайт]. – 2019. – 22 окт. – URL: https://www.thoughtco.com/psychological-warfare-definition-4151867 (дата обращения: 27.04.2022).

8. Theohary, C. A. Information Warfare: Issues for Congress / C. A. Theohary // Congressional Research Service : официальный сайт. – 2018. – 5 марта. – URL: https://sgp.fas.org/crs/natsec/R45142.pdf (дата обращения: 28.04.2022).

9. Libicki, M. C. What Is Information Warfare? / M. C. Libicki // Strategic Forum : materials of the 28th forum / National Defense University, Institute for National Strategic Studies. – Washington, DC, 1995. – P. 2-4.

10. Bishop, M. The strategy and tactics of information warfare / M. Bishop, E. Goldman // Contemporary Security Policy. – 2003. – Vol. 24, Iss. 1. – P. 113-139.

11. Cyberspace Operations JP-3–12 // Joint Chiefs of Staff. – 2018. – 104 p. – URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (дата обращения: 1.05.2022).

12. Qureshi, W. A. Information Warfare, international law, and the changing battlefield / W. A. Qureshi // Fordham Int'l LJ. – 2020. – Vol. 43, Iss. 4. – P. 901-938.

13. Damjanović, D. Z. Types of information warfare and examples of malicious programs of information warfare / D. Z. Damjanović // Vojnotehnički glasnik. – 2017. – Vol. 65, Iss. 4. – P. 1044-1059.

14. Schleher, D. C. Electronic warfare in the information age : advanced practitioner's guide / D. C. Schleher. – Norwood : Artech House Publishers, 1999. – 624 p. – ISBN 0-89006-526-8.

15. Wik, M. W. Revolution in information affairs: Tactical and strategic implications of Information Warfare and Information Operations / M. W. Wik, A. Jones, G. L. Kovacic, P.G. Luzwick // Global information warfare. – 2002. – P. 579-628.

16. Курюхин, А. Н. Цифровые технологии в выборных процессах как вызов перспективам демократии / А. Н. Курюхин // Власть. – 2019. – №. 3. – С. 63-67.

17. Маркова, А. В. Последствия и перспективы применения кибератак как инструмента внешней политики государств на примере вируса «Стакснет» / А. В. Маркова // Актуальные проблемы гуманитарных и естественных наук. – 2014. – №. 2-2. – С. 297-302.

18. Уварова, А. Опасность и безопасность — гонка виртуальных вооружений / А. Уварова // Хабр : [сайт]. – 2016. – 27 окт. – URL: https://habr.com/ru/post/313460/ (дата обращения: 18.05.2022).

19. Global Digital 2022: вышел ежегодный отчёт об интернете и социальных сетях — главные цифры // Sostav : [сайт]. – 2022. – 28 янв. – URL: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472.html (дата обращения: 17.05.2022).

20. Сарна, А. Я. Технологии воздействия на аудиторию в современном медиапространстве / А. Я. Сарна // Вестник Санкт-Петербургского университета. Социология. – 2020. – Т. 13, №. 2. – С. 218-235.

21. Якимчук, В. В. Понятие гибридной и информационной войн в российской и зарубежной литературе / В. В. Якимчук // Скиф. Вопросы студенческой науки. – 2020. – №. 8 (48). – С. 161-167.

22. Медовкина, Л. Ю. Эволюция информационных войн от древности к современности / Л. Ю. Медовкина // Известия Тульского государственного университета. Гуманитарные науки. – 2017. – №. 3. – С. 15-24.

23. Шариков, П. А. Информационные операции в современной военной стратегии США. Анализ доктринальных документов министерства обороны и государственного департамента США / П. А. Шариков // Россия и Америка в XXI веке. – 2015. – №. 1. – С. 4.

24. Под Киевом слышны взрывы // ТАСС : [сайт]. – 2022. – 24 февр. – URL: https://tass.ru/proisshestviya/13825933?utm_source=google.ru&utm_medium=organic&utm_campaign=google.ru&utm_referrer=google.ru (дата обращения: 17.05.2022).

25. Минобороны РФ сообщило о нанесении ударов по военной инфраструктуре Украины // INTERFAX.RU : [сайт]. – 2022. – 24 февр. – URL: https://www.interfax.ru/russia/824028 (дата обращения: 18.05.2022).

26. В посольстве России назвали действия Meta объявлением информационной войны без правил // ТАСС : [сайт]. – 2022. – 11 марта. – URL: https://tass.ru/politika/14035157 (дата обращения: 19.05.2022).

27. Зеленский поблагодарил Meta за призывы к насилию против россиян // РИА Новости : [сайт]. – 2022. – 13 марта. – URL: https://ria.ru/20220313/meta-1777961498.html (дата обращения: 18.05.2022).

28. "СПАСАТЕЛИ, ТЕЛА, ЛЮДИ В ГОРЕ": ЗАХАРОВА ПОКАЗАЛА "БОЙНЮ" В СМИ // chita.tsargrad.tv : [сайт]. – 2022. – 17 марта. – URL: https://chita.tsargrad.tv/news/spasateli-tela-ljudi-v-gore-zaharova-pokazala-bojnju-v-smi_512981 (дата обращения: 16.05.2022).

29. Тела в Буче, роддом в Мариуполе, обстрел театра: борьба с фейками продолжается // Краснодарские известия : [сайт]. – 2022. – 6 апр. – URL: https://ki-news.ru/2022/04/06/tela-v-buche-roddom-v-mariupole-obstrel-teatra-borba-s-fejkami-prodolzhaetsya/ (дата обращения: 18.05.2022).

30. Фейк: в Мариуполе был атакован роддом // войнасфейками.рф : [сайт]. – 2022. – 10 марта. – URL: https://войнасфейками.рф/civil/fejk-v-mariupole-byl-atakovan-roddom/ (дата обращения 17.05.2022).

31. Совина, М. Небензя фотографиями опроверг «авиаудар» России по роддому в Мариуполе / М. Совина // Lenta.ru : [сайт]. – 2022. – 12 марта. – URL: https://lenta.ru/news/2022/03/12/nebenzya/ (дата обращения: 16.05.2022).

32. Безменов, А. Журналист назвал провокацию в Буче началом информационной войны против России / А. Безменов // ИА «ДОН24» : [сайт]. – 2022. – 4 апр. – URL: https://don24.ru/rubric/politika/zhurnalist-nazval-provokaciyu-v-buche-nachalom-informacionnoy-voyny-protiv-rossii.html (дата обращения: 15.05.2022).

33. Чернышова, Е. Постпред при ООН заявил об 1,2 млн «порочащих военную операцию» фейков / Е. Чернышова // РБК : [сайт]. – 2022. – 28 февр. – URL: https://www.rbc.ru/politics/28/02/2022/621bf5919a79471fce7f5644 (дата обращения: 18.05.2022).

34. Шубин, Д. В. Роль медиаконтента в информационном противостоянии государств (на примере «Сирийского конфликта») / Д. В. Шубин // Актуальные проблемы мировой политики : материалы V ежегодной международной научной конференции молодых ученых / Дипломатическая академия

Министерства иностранных дел Российской Федерации. – Москва, 2019. – С. 52-60.

35. А был ли мальчик? Самые громкие фейки сирийской войны // РИА Новости : [сайт]. – 2017. – 17 марта. – URL: https://ria.ru/20170317/1490291805.html (дата обращения: 19.05.2022).

36. Springer, P. J. Cyber Warfare: A Documentary and Reference Guide / P. J. Springer. – Santa Barbara, CA : Greenwood, 2020. – 357 p. – ISBN 978-1-4408-7278-5.

37. Шинкарецкая, Г. Г. Международное космическое право и юридические лица / Г. Г. Шинкарецкая // Труды Института государства и права Российской академии наук. – 2020. – Т. 15, №. 1. – С. 59-80.

38. Стрельцов, А. А. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству / А. А. Стрельцов // Право и государство: теория и практика. – 2014. – №. 3. – С. 75-88.

39. Аксенов, А. Б. Всеобщая декларация прав человека и проблема универсализации прав человека / А. Б. Аксенов // Вестник экономики, права и социологии. – 2018. – №. 1. – С. 59-62.

40. Орлов, А. С. Концепция общего наследия человечества и ее влияние на развитие международного права / А. С. Орлов // Вестник Удмуртского университета. Серия «Экономика и право». – 2017. – Т. 27, №. 6. – С. 99-106.

41. Нараева, А. ООН просят устанавливать цифровой нейтралитет в период вооруженных конфликтов / А. Нараева // Ведомости : [сайт]. – 2022. – 8 марта. – URL: https://www.vedomosti.ru/society/articles/2022/03/08/912604-oon-tsifrovoi-neitralitet (дата обращения: 20.05.2022).

Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
**«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

Юридический институт

кафедра международного права

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т.Ю. Сидорова
подпись инициалы, фамилия
«25» мая 2022 г.

# БАКАЛАВРСКАЯ РАБОТА

41.03.05. Международные отношения

Информационные войны в медиа-пространстве

Руководитель 24.05.22 доцент, к.ю.н Э.А. Павельева
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник 24.05.22 К.В. Рубан
подпись, дата инициалы, фамилия

Красноярск 2022