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 технологии в современных международных отношениях

Руководитель	_____	профессор, д.и.н	Е.В. Мороз
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	_____		Ю.В. Пьянкова
	подпись, дата		инициалы, фамилия

Красноярск 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время, наш мир находится в состоянии технологической революции, трансформации, двигателем которой стали информационные технологии. Для данного явления характерно не только огромное поле Расширяясь в своем влиянии все больше, информационные технологии способны повлиять на государства и их внешнюю политику. Соединенные Штаты Америки и их союзники с помощью современных информационно-коммуникационных технологии проводят курс давления на политику, экономику, информационную сферу Российской Федерации, что непосредственно приводит к возникновению кризиса на международной арене.

Одним из самых уникальных и интересов аспектов в информационных технологиях является исследование мегатрендов информационной эры, поскольку наравне с данными, приводимыми Международным союзом электросвязи об измерении уровня информационного развития общества и показатель прогресса информационно-компьютерных технологий в различных государствах мира, исследуются явления «Интернет вещей», технология «блокчейн», к примеру, драйверы Industry4.0. Существенный научный интерес вызывает также анализирование перспектив и опасностей, которые лежат в применении НБИК-технологий и искусственного интеллекта для сети национальной и международной безопасности [7].

В настоящее время идет детальная проработка практических и теоретических паттернов применения современных информационных технологий в качестве «мягкой силы 2.0» государствами-лидерами на международной арене, включая исследования влияния и использования соцсетей в дипломатической практике Оксфордского университета [12], а также разных технологий спекуляций и цифровых фейковых новостей в ходе информационных войн. Беря в расчет возрастание конфликтного потенциала в современном мире, целесообразно подчеркнуть актуальность обзоров

ситуационно-кризисных центров российских и зарубежных внешнеполитических ведомств, сначала может показаться самым рациональным решением, соответствующим всем требованиям сложившейся обстановки, однако, при более подробном изучении можно увидеть целый ряд серьезных проблем. Это относится не столько к сфере кибербезопасности, а еще к тому, что в информационную эпоху почти все виды соперничества между государствами перешли в цифровую среду – в особенности, это касается экономической борьбы, а также используемых в таких конфликтах информационно-аналитических, геоинформационных и иных систем, включая когнитивный анализ и прогнозирование течения международных конфликтов.

С постоянно растущим напряжением в международных отношениях, заинтересованному лицу принесет пользу исследование и анализирование сферы информационной в дип. практике с учетом главных статей и пунктов Доктрины информационной безопасности Российской Федерации (2016) [16], Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (2017) [65], Системы центров реагирования на компьютерные инциденты (CERT) [85] и Системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России (СОПКА) [65].

Стоит отметить, что Министерство иностранных дел Российской Федерации и его загранучреждения все больше и чаще подвергаются компьютерным и информационным атакам, и именно по этой причине необходимо исследовать такие практические аспекты, как методы борьбы с бот-нетами, вирусами, шпионскими программами, цифровыми фейками и т. д.

Поскольку одной из главных тенденций развития человечества на современном этапе является преобразование социальных сфер под влиянием информационной революции, необходим комплексный подход к исследованию проблем в международных отношениях политического и правового характера,

возникших под влиянием информационных технологий, и именно это и обуславливает **актуальность** темы.

Объектом исследования являются информационные технологии в современных международных отношениях.

Предмет исследования — основные направления и факторы воздействия информационных технологий на современные международные отношения.

Целью работы является детальное изучение теоретических и практических основ, а также влияния информационных технологий на международной арене, а затем – последующий анализ его воздействия на взаимоотношения между государствами и на международные отношения в целом.

В ходе работы предстоит выполнить следующие **задачи:**

- Проследить взаимосвязь определений «информационные технологии», «информационная безопасность»;
- Проанализировать направление развития и воздействия фактора информационных технологий на мировую политику;
- Изучить и охарактеризовать международно-правовое регулирование современных информационных технологий;
- Рассмотреть классификацию и содержание киберпреступлений в международном праве;
- Проанализировать инициативы Российской Федерации по обеспечению международной информационной безопасности в ОНН в современных международных отношениях;
- Проанализировать сотрудничество Российской Федерации с международными и региональными организациями по обеспечению международной информационной безопасности.

Степень научной разработанности: Влияние информационных технологий на международные отношения изучали С.И.Долгов [18], Е.И.Поверинов[40], П.А.Цыганков[71]. В научной литературе широко известны

работы по политическим аспектам информационной безопасности И.Н.Панарина[38].

Свой вклад в изучение электронной демократии и влияния информационно-коммуникационных систем на международные отношения также внесли Р. Дэвис[77], А. А. Чесноков[72], Дж. В. Дейк[78], К. Хакер[80], Л. А. Василенко[6] и многие другие научные специалисты.

Исходя из целей и задач исследования были использованы следующие **методы**: исторический, социологический, сравнительно-правовой, а также функциональный.

По **структуре** работа состоит из введения, трех глав, заключения и списка использованных источников. Во ведении описана характеристика работы, ее актуальность, определяются цели и задачи исследования, а также дается обзор разработанности темы исследования. Первая глава посвящена терминологии, которая используется при описании информационных технологий, а также влияние информационных технологий на современность. Во второй главе приведен сравнительный анализ нормативно-правовых актов, которые регулируют информационные технологии. Третья глава посвящена сотрудничеству Российской Федерации с разными странами и международными организациями по обеспечению международной информационной безопасности. В заключении вынесены все основные выводы по итогам исследования.

ГЛАВА I. Информационные технологии: понятие, подходы в теории международных отношений

1. Терминология и понятия информационных технологий

Данное научное исследование лежит в анализе информационных технологий как одного из основных факторов влияние на международной арене. Поскольку литература политического и социологического характера, международно-правовые документы, национальной законодательство разных стран по-разному обозначают термины одного и того же явления, прежде всего стоит рассмотреть именно аспекты терминологии, ведь именно от научного термина будет зависеть, каким содержанием заполнится, а это будет влиять на сужение или расширение границ исследования.

Прямая связь лежит между терминологией и «проблемой определения». В первую очередь, процесс определения начинается из конкретной ситуации, когда объект, которому предстоит этот термин дать, изучается именно с точки зрения потребности этого исследования, в котором ищут определение для этого явления или объекта. Соответственно, при отсутствии какой-либо конкретики, попытки просто идентифицировать, дать определение объекту в общем смысле приведут к определениям без необходимого уровня информативности. Более того, не раскрывая терминологическое значение, решать проблему определения просто нельзя – ведь интерпретация определенных терминов(к примеру, «информация») это лишь один из вариантов трактовки, разные ученые в разное время приводили свое видение того или иного слова [3]. Так что, если исследование характеризуется двумя вышеизложенными пунктами, оно зайдет в тупик и не будет носить позитивный характер.

Таким образом, можно сделать вывод, что при изучении вопроса терминологии в области информационных технологий, необходимо не просто перечислять термины из теоретических, практических и законодательных

положений, но и подробнее рассмотреть их содержание, иными словами, дать им определение.

В содержании данного раздела следует рассмотреть ряд терминов и понятий, а также проанализировать их характеристики, ведь это непосредственно влияет на изучение фактора влияния информационных технологий на международные отношения.

Использование того или иного термина предусматривает анализ его содержания из различных научных областей, чтобы понять его истинный смысл.

Сейчас государства особенно заинтересованы в исследованиях о природе информации и данных. Именно поэтому в данной главе мы рассмотрим информацию с разных точек зрения.

Как уже давно известно, информация – это новейший и актуальнейший предмет изучения, а также объект особой важности, подлежащий контролю со стороны государства. Так как теперь данное явление представляет собой ключевой элемент жизни человека, а также изучается огромным количеством ученых по всему миру, имеет смысл рассмотреть его понимание в общей науке, в правовом значении, в кибернетике и, конечно же, в социологии, ведь это, вне всякого сомнения, касается нашего общества.

Как и количество сфер, касающихся информации, достаточно большое, так и понятий данного слова – немыслимое множество. Имеет смысл обратиться к основным из них. Классическое толкование любого слова мы можем найти в Большом энциклопедическом словаре [4]. Согласно словарю, информация имеет несколько граней и смысл зависит не только от контекста, но и от лица, которое употребляет данное слово. Так, мы можем найти толкование информации с бытовой, научной, социологической и кибернетической точек зрения.

Как определил один из кибернетических гениев и основоположников Норберт Винер, информация – это определенный набор сигналов, которые мы

получаем из внешнего мира, перерабатываем и транслируем на внешний мир [9].

Нельзя упускать из внимания и К. Шеннона. Его вклад в кибернетическое развитие не менее огромен, чем у вышеупомянутого Норберта Винера, и этот научный специалист видел информацию как некое сообщение, которое способно возвести или разрушить стену недосказанности [73].

Есть источники, которые толкуют информацию с одной определенной точки зрения. Например, только с социологической или технической. Так, в Толковом словаре мы увидим, что информация — это ничто иное как технологический термин, обозначающий массив данных. Эти данные передает машина или компьютер, выдавая информацию, которую дальше обрабатывает человек. Данное пояснение звучит вполне обосновано, так как машина не способна обработать содержание информации самостоятельно, а лишь проецирует те смыслы, которые запрограммировал человек. В этом и есть главное различие между технологиями и человеком [4].

Некоторые авторы приписывают информации лишь биологический характер, называя информацию набором чувств, с помощью которых мы собираем информацию из внешнего мира в виде определенных материй и энергии. [41].

Если обращаться к отечественному пониманию, то следует взять во введение тот факт, что в российском праве самое старое и первое определение термина «информация» прописано в Законе об информации от 1995г. [64], во второй статье говорится, что информация — это «сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления». Действующий российский закон определяет информацию как массив данных, которые не ограничиваются определенной формой [63].

Перед анализом терминов в международных актах, следует обратить внимание на тот факт, что термин «информация» в международно-правовых документах требует особой осторожности в изучении по ряду причин.

Основная особенность заключается в том, что большинство международных документов написаны на английском языке.

В данном лингвистическом направлении термин «data» употребляется, чтобы обозначить как информацию, так и данные.

Соответственно, чтобы более детально проанализировать употребление понятия «информация», следует исследовать только понятие «information». Тем не менее, можно встретить такие ситуации, где из контекста становится ясно, что и термин «data» употребляется в значении «информации». В таком варианте можно использовать оба обозначения.

Если постараться найти отличия в использовании двух этих понятий, то можно более четко выделить, где лежит грань между «данными» и «информацией».

В странах-членах СНГ (Содружества Независимых Государств) определение «информации» было лишь совсем немного преобразовано и адаптировано под постсоветское понимание. Мы видим, что данные это — «сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их регистрации и представления», как это интерпретирует и поясняет Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ стран-участниц СНГ в сфере информатизации от 24 декабря 1999 г. в г. Москва [5].

Что касается международно-правовых актов, то в них дефиниции информации не обозначены [26]. В свою очередь, термин «данные» — это родственное понятие по отношению к «информации».

Очень часто в различных исследованиях и научных трудах можно встретить объяснение, что «данные» сами по себе представляют такие сведения, которые человек извлекает через измерение, наблюдение и других научных методов получения необходимых ему составляющих, а затем

показывает их в той форме, которая сгодится для хранения на постоянной основе, а также обработки автоматизированными системами.

Соответственно, если сравнивать «информацию» и «данные», то невооруженным взглядом можно заметить очевидный факт. «Информация» сама по себе намного шире, разностороннее как термин, нежели ее родственная дефиниция «данные». И главное отличие, на самом деле, заключается в одной простой вещи и масштабах, которых касаются определения. Информация – это любые сведения, а данные – только те, которые получены с помощью определенного инструмента или махинации и которые можно сохранять на долгосрочной основе.

Поскольку в данной работе изучается именно воздействие со стороны информационных технологий на международные отношения, то и рассматривать имеет смысл именно нормативное понятие в контексте информационных и компьютерных данных. В Конвенции о киберпреступлениях данные определяются как определенные части информации, которые должны быть обработаны компьютером. Причем такие данные могут быть в любой форме, даже в виде определенного программного обеспечения, которое может воздействовать на компьютерные системы.[1]

Далее следует перейти к такому понятию, как «информационная система». Следует подчеркнуть, что оно актуально абсолютно для каждой сферы жизни социума, а в контексте международных отношений, приобретает особое значение и содержание.

Несмотря на то, что международные отношения могут переходить в спонтанное течение, основным способом их протекания являются действия по воле правительства государств, а их конечной целью в таком случае является достижение того или иного результата. Соответственно, как и гражданские отношения, отношения на международной арене представляют собой скорее

[1] Подписана 23.11.2001г. в Будапеште. Конвенция вступила в силу 01.07.2004г. Россия приняла решение подписать Конвенцию с заявлением (Распоряжение Президента РФ от 15.11.2005 N 557-рп)

совокупность событий и фактов, результатом которых всегда становится определенные юридические и политические последствия.

Точкой отсчета в изменения международной обстановки в целом или же международно-политической ситуации считается принятие решение внешнеполитического характера со стороны актора, субъекта международных отношений.

Актору международных отношений необходимо обладать достоверной информацией, чтобы принять своевременное, качественное решение, соответствующее его потребностям и интересам. Само по себе его решение – это действие, проявляющее волю актора, которое вступает в силу после обработки и оценки той информации, которой обладает субъект международных отношений.

В Российской Федерации «информационная система» определена в Законе об информации как «совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств» [66].

Одновременно с этим можно наблюдать, что вышеуказанные дефиниции не совсем полны относительно содержания понятия «информационная система» и носят довольно узкий характер. На самом деле, «информационные системы» в принципе шире, чем многие другие термины, и как уже говорилось ранее, дефиниции в этой области разноплановые, поэтому и это определение можно рассматривать не только как какие-то данные или множество сведений, но и те технологии, которые их обрабатывают. Очень часто в глобальных масштабах информационные системы связывают с мировой системой информационных технологий, в состав которой входят информационный источники, технические средства, и все это связывает в единую сеть для передачи, обмена, хранения, обработки и создания информации.

Далее стоит перейти к следующему понятию, которое имеет прямую связь с информационной системой, - «информационная среда».

«Информационная среда» — это такая область общественной деятельности, которая является составной частью социальной среды, она обуславливается большой ролью информации и влияния информационных технологий на человеческую деятельность, в которой субъекты обмениваются данными с помощью носителей информации. Информационная среда бывает национальной и глобальной.

Та информационная среда, которую считают глобальной, состоит из субъектов (системы, организации), вовлеченных в процесс сбора, обработки и распространения информации как на международном, так и национальном уровнях.

Современная обстановка сложилась таким образом, что главными участниками в информационной среде являются СМИ. Как правило, они либо актуализируют и внедряют собственные концепты, либо стараются проводить объективную деятельность. Их количество постоянно растет, как и роль на международном поприще, и ключевую роль в данном процессе играют как раз информационные средства и глобальная сеть Интернет.

В международной практике также часто используют такой термин, как «киберпространство». Его наипростейшее понимание – это «пространство, в котором взаимодействуют электронные объекты» [81]. Однако, исследователи данного вопроса могут столкнуться с таким моментом, что это трактование имеет слишком широкий смысл и не является достаточно конкретизированным и глубоким, за что и подлежит критике со стороны приличного количества деятелей.

Такой термин, как «киберпространство» впервые использовала Анжелика Артюх, в свое время являвшаяся известной писательницей. Она полагала, что каждый «компьютер существует в консенсусе с нервной системой своего пользователя» [2]. Писательница говорила о том, что киберпространство — это некое место, в котором вся в мире информация переплетена и объединена между собой. И посетить это место может только нечто без тела и

разума. Сейчас мы понимаем, что такие рассуждения больше похожи на облачные сервера и компьютеры.

Вся ее теория представляла собой бесконечный информационный поток, которые изменяется не только по содержанию, но и визуально. Так Артюх представила киберпространство, где абсолютно каждое звеное соединено между собой сотнями связей[2].

Тем не менее, данное понимание не является единственным. Оппозиционная точка зрения заявляет, «киберпространство является интернациональным, и на него не распространяется государственный суверенитет» [76].

Вдобавок к вышенаписанному мнению, научный деятель Д. Барлоу выразился, что киберпространство – это экстерриториальное явление вне влияния государственных законов и правовых систем в принципе [74].

Также существует точка зрения, что киберпространство – это научное понятие без каких-либо рамок и ограничений, а смысл термина боле походит на метафору, который не требует дополнений или объяснений. Данный взгляд нельзя обозначать ошибочным – ведь в целях регуляции как со стороны государства, так и международного сообщества, следует найти точное, полностью отображающее смысл определение киберпространства.

В особенности это касается трактования в рамках права, ведь именно оно в будущем повлияет на объективную оценку неподобающего поведения на поле информационной среды.

Таким образом, изучив наиболее распространенные и важные понятия для темы исследования, можно сделать вывод, что терминология информационных технологий еще не устоялась и только начала оформляться как таковая, потому что данная сфера, на самом деле, все еще является довольно новой.

В будущем, с дальнейшим развитием информационных технологий в международных отношениях и в общем, данная проблема обязательно будет разрешена и потребует нового рассмотрения, более детального и подробного.

2. Общее направление развития и воздействия фактора информационных технологий на мировую политику

С возникновением информационных технологий и распространении их по всему земному шару, в большинстве стран появились условия для формирования новый коммуникационных связей.

Традиционные институты общества – экономические, научные, политические – под влиянием информационных технологий стали эволюционировать, вовлекать в свою работу интернет-ресурсы и современные технологии. Теперь информационные технологии, как уже было упомянуто ранее, присутствуют в жизни человека повсеместно – как в его повседневных делах, так и образовании, и работе.

Это не могло не затронуть и политические аспекты – информационные технологии на данный момент являются объектом международных отношений и ведущим фактором развития, причем довольно специфическим и многогранным – для информационных технологий характерные технические, политические, социальные явления.

Как показывают исследования Министерства торговли Соединенных Штатов, радио за тридцать лет достигло пятидесятимиллионной аудитории, телевидение – за тридцать, а Всемирная Сеть Интернет – всего лишь за четыре года [55].

Благодаря Интернету каждый гражданин может участвовать как во внутренней политике своего государства, так и во внешней. Это также касается

формирования идеологии страны, стратегических решений (к примеру, включение в состав страны еще одного субъекта и др.)

Как указывает социолог Говард Рейнгольд: «Ценность интернета повышается в квадратичной пропорции по отношению к числу узлов в интернете» [44]. Иными словами, если количество интернет-пользователей увеличится в два раза, то возможности Интернета вырастут в четыре.

Чтобы более подробно разобрать процесс воздействия информационных технологий, следует рассмотреть ключевые элементы международной системы сетевого пространства:

- сервера, кабели, спутники, пропускающие интернетный трафик и являющиеся связующим компонентов;
- системы поиска – к примеру, Яндекс в Российской Федерации;
- гейты и периферийные структуры, с помощью которой телекоммуникационные сети – GSM – встроены во Всемирную паутину;
- домены и их адреса, фиксирующие положения сайтов в Интернете, как правило, они поддерживаются согласием провайдеров.

В политической сфере помимо перечисленных аспектов также имеют значение и несетевые факторы, такие, как программное обеспечение или технологические решения на основе информационных технологий, приводящие к существенным сдвигам в промышленной области. Благодаря постоянному прогрессу информационные технологии охватывают все большую долю в организации работы органов власти.

В зарубежном опыте следует рассмотреть американские и британские электронные государственные службы. В первую очередь, они проводятся в открытом доступе и подлежат подотчетности институтам гражданского общества. Это заключается не только в передаче данным гражданским лицам, но также и к перечислению занятых в данном вопросе госучреждений. Таким образом, данные о показателях становятся доступными для обычных людей, и

каждый может оценивать их самостоятельно, базируясь на собственных взглядах, а не на заявлениях официальных лиц [88].

Помимо этого, информационные технологии воздействуют не только на внутреннюю, но и на внешнеполитическую деятельность государств, включая дипломатическую практику. Одним из последствий такого влияния является отход традиционных методов борьбы на второй план и замена их информационными войнами и сетевыми атаками. Конечно, международные конфликты все еще не прекратили существование в вооруженной форме, но теперь они сопровождаются и такими явлениями, и даже в мирное время такого рода гонки между государствами продолжают идти [88].

В теории, вполне вероятен исход, что вооруженная борьба будет заменена информационным воздействием целиком, и геополитические конфликты смогут быть разрешены без человеческих жертв.

Информационные технологии имеют огромный потенциал для перестройки архитектуры международной системы в принципе, не только в форме атаки, но и взаимодействия – информационные технологии позволяют устанавливать связь между лидерами стран, проводить переговоры и конференции международного уровня в сетевом, онлайн формате, таким образом не затрачивая время людей на длительные перелеты и оформление необходимых транзитных документов [79].

Таким образом, становится очевидно, что информационные технологии нуждаются в международном правовом регулировании, которое на настоящем этапе существенно отстает от уровня развития информационных отношений.

Не менее важными являются моменты, касающиеся международно-правовой безопасности.

Как утверждал Анатолий Васильевич Торкунов [57], российский историк, дипломат и политолог, все множество информационных ресурсов государств, их программные обеспечения, базы данные, сети информации – это как сильнейшие инструмент в ходе информационной борьбы, так и в принципе

объект влияния со стороны врага. Поэтому весьма вероятен тот опасный для общества исход событий, где для удовлетворения своих военно-политические интересов в борьбе за первенство на международном поприще, государства могут массово начать использовать весь мощнейший потенциал информационных технологий во вред своим оппонентам. Не секрет, что развитые страны регулярно повышают свой военный потенциал именно благодаря новым информационно-кибернетическим разработкам, что заставляет пресловутый баланс сил просто разрушаться на глазах, а формы противостояния и борьбы – увеличиваться и совершенствоваться. Государства становятся вольными или невольными участниками киберугроз в виде хакерских атак, информационных войн, фейковых новостей, и таким образом понимание агрессии расширяется, преобразуется и становится новым.

Соответственно, возрастает необходимость к основным аспектам повестки дня вопроса о контроле военной деятельности с акцентом на информационные технологии. Сейчас становится ясно, что информационные технологии в определенный этап развития могут стать угрозой для мирового сообщества.

Здесь же возникает проблема прав человека – информационные технологии вовлекают в себя свободу слова, доступ к информации, приватность, дезинформацию и свободу коммуникации.

С внедрением информационных технологий в международные отношения, в мировой политике возникло новое явление, получившее название «межгосударственные альянсы». Они формируются вокруг информационных интересов и берут за базис своей деятельности обеспечение доступа к определенной технологии и проведение единой информационной мировой политики. Фактически, это может быть новый вид политических союзов. Кроме того, они возникают не только на международном, но также региональном и национальном уровнях.

Еще одним последствием информационного влияния стали «информационные санкции», новые вид политического воздействия, уже вполне доказавшие свою эффективность [35].

Возникает и электронная международная торговля. Согласно данным Конференции ООН по торговле и развитию [27]: «В период с 2020 по 2021гг. онлайн-торговля в глобальной сети Интернет достигла показателей 12 трлн. долларов». Тем не менее, несмотря на прослеживающийся прогресс, проблемные аспекты все еще существуют – к примеру, вопрос налогообложения.

Электронная экономика сама по себе не только обеспечивает трудовые отношения в дистанционном форме, но и предоставляет возможность более эффективного использования ресурсов и вовлекает все больше членов общества в данную деятельность.

С дальнейшим информационным развитием отдельные страны мира могут увеличить производительность своей экономики на мировом рынке, быть вовлеченными в процессы интеграции. Это все указывает на факт, согласно которому каждому государству нужно развивать информационную инфраструктуру на национальном уровне, не забывая о вкладах в формировании «глобального информационного общества». Главная идея – найти и удержать этот необходимый баланс.

Существует идея о том, что в ближайшем будущем из-за информационного прогресса и разных взглядов на этот процесс с точки зрения менталитетов государств, международные отношения могут войти в новый вид конфликта – информационное неравенство, «digital divide».

Как полагают представители Института мировых ресурсов (World Resources Institute): информационное неравенство или же digital divide тормозит и замораживает развитие информационных технологий как для государств, так и для международных организаций, т.е. негосударственных акторов Виной тому – разрыв в технологическом развитии между развитыми странами и

беднейшими странами третьего мира, который постоянно прогрессирует. Как говорят некоторые сведения, лондонцы имеют больше аккаунтов в Интернете, чем африканские жители в целом, а до восьмидесяти процентов всего населения земли вообще никак не связаны с глобальными коммуникационными сетями [89].

Вдобавок к этому журналист М. С. Вершинин [1] выдвигает собственную экспертную версию. Он говорит о том, что одна пятая часть населения Земли это активные пользователи сети Интернет.

Соответственно, можно сделать вывод, что неравноправие в вопросе информационного доступа влияет на все остальное неравенство в мире, как в глобальных масштабах между государствами, так и на локальном между социальными группами в одном государстве.

Международное сообщество активно работает над решением данной проблемы. Первый документ, зафиксировавший понятие цифрового разрыва и право всех людей на доступность информационных технологий, был подписан в июле 2000 г. в Окинаве, Япония. Он носит название «Хартия глобального информационного сообщества» [35].

Фактически, данное соглашение стало программным документом для построения глобального информационного общества и подготовки Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО).

На современном этапе пристальное внимание данной проблеме уделяет ЮНЕСКО, «ведущий разработку и реализацию концепций преодоления цифрового разрыва» [75].

Российская Федерация проявила инициативу в создании международных документов по данному вопросу и закреплении там приоритетов по международной стабильности и безопасности, а также создании международных центров коллективного доступа к информационным технологии, в том числе, в отдаленных районах.

Позиция России выражает идею о том, что глобальное информационное общество может быть создано только на основе международной безопасности, национального суверенитета, борьбы с международным информационным терроризмом и информационной преступностью.

Как можно увидеть, в настоящее время большинство международных организаций включили информационные технологии в свою работу.

Таким образом, можно сделать выводы на основе изученного материала, что информационные технологии в действительности обширно влияют на международные отношения, причем не только на традиционные их формы, но и сетевые.

Конечно, воздействие такого уровня всегда двояко.

Из положительных аспектов можно выделить демократизацию мировой политики, возникновение новых игроков на международной арене, установление обширной сети коммуникационных связей по всему миру и более удобный процесс взаимодействия граждан с государственными организациями в своей стране.

Но существуют и информационные нарушения – киберпреступность, международный информационный терроризм, фейковые новости и т. д., в целях снижения которых некоторые государства ограничивают доступ к информационным технологиям, что однозначно негативно сказывается на уровне жизни и совершенствования гражданского общества.

Конечно, в Интернет-сети действительно нельзя отрицать существование взаимодействия друг с другом террористических группировок, наркокартелей и других нарушающих международную безопасность организаций, но это должно вести к модернизации регулирования интернет-безопасности и сохранности данных, а также методов расследований в сетевом пространстве, а не к полному запрету информационных технологий в принципе.

Соответственно, информационные технологии в настоящее время – главный двигатель прогресса и международная угроза в одно и то же время, но

для борьбы с такими вещами суть проста: «с информационными угрозами нужно бороться информационными методами».

ГЛАВА II. Международно-правовое регулирование современных информационных технологий

1. Международно-правовые основы регулирования отношений в сфере информационных технологий

Для того, чтобы исследовать информационные технологии как фактор воздействия на международные отношения, необходим комплексный подход с точки зрения сразу двух наук – международных отношений и международного права, ведь это две смежные научные области, схожие в своих роде и проблематике. Разумеется, что несмотря на всю свою связанность и схожесть, они выступают отдельными научными сферами, но что касается проблем, связанных с ними, то нельзя изучить данные аспекты с точки зрения только какой-то одной науки. Рассматривая проблемы международного права, исследователи всегда обращаются к международным отношениям, и наоборот. Информационные технологии не являются исключением [70].

Как уже было рассмотрено ранее, информационная сфера на международном уровне стала более урегулированной, включая контроль с помощью правовых способов. Одним из более ярких примеров можно назвать «компьютерный сбой тысячелетия» 2000 года, во время которого государства сотрудничали между собой, чтобы разрешить данный вопрос, ведь информационное поле и технологии отдельных стран представляют собой большую «паутину», где все взаимосвязано.

Чтобы более подробно понять данный аспект, нужно обратиться к анализу международно-правовой базы информационной безопасности, а также угроз в киберпространстве, и в первую очередь – определить место международного права в информационных отношениях государств.

Сами по себе источники международного права делятся на две группы – основные (договоры и обычаи на международном уровне) и вспомогательные (документы международных организаций, решения судов и доктрины).

Международные договоры являются основными и главными источниками международного права, которые представляют собой определённые соглашения между государствами. Венская Конвенция о праве международных договоров [8] дает нам очень конкретное и понятное определение международному договору. А именно это письменное соглашение между государствами, которое регулирует международное право. Важно, что соглашение между государствами может быть заключено в нескольких документах, однако, все они будут связаны между собой.

Следует отметить, что документа, регулирующего все аспекты, связанные с информационными технологиями, в настоящее время просто нет. Поэтому существуют различные международные акты в информационной сфере. Особенно важными считаются те, которые содержат нормы уголовного международного права.

На глобальном уровне в рамках «Группы восьми» в июле 2000 года приняла такой акт, как Окинавская хартия глобального информационного общества [82]. К документу, регулирующему кибербезопасность, присоединились те страны, которые осознают и определяют необходимость движения всего мирового сообщества к информационному обществу. Дополнительно на Окинавском саммите была создана «Группа по возможностям цифровых технологий» [35] («Digital Opportunity Task Force», «DOT Force») — организованное сообщество, которое занимается проблемой «цифрового разрыва».

Согласно документу, прежде всего, глобальное информационное общество будет стабильно лишь при развитии ведущих принципов демократии – свободы в информационном обмене, толерантности, уважения друг к другу. Также подчеркивается важность нахождения правовых решения вопроса информационного неравенства, ведь Хартия обозначает доступность информационных технологий для каждого человека одной из главных целей.

Первым случаем в истории международных отношений относительно всецелого урегулирования проблемы преступлений с использованием компьютерных технологий была попытка Организации экономического сотрудничества и развития (ОЭСР) - организации, появившейся на основе Организации европейского экономического сотрудничества, в свою очередь учрежденной в далеком 1961 году для перераспределения ресурсов помощи на послевоенное восстановление Европы от Канады и США (План Маршалла). В своей работе Организация руководствуется идеей о построении «здоровой экономики» в странах участницах – иными словами, усовершенствовать эффективность экономики, связать между собой рыночные системы государств, распространить влияние таких ценностей как экономическая свобода, а также осуществлять вложения в развитие как развитых, так и развивающихся стран. ОЭСР эксперты часто называли «научным центром, контролирующим органом, клубом богатых стран, практическим университетом», и каждое из данных определений валидно, тем не менее, они не отражают всей сути института, в который входят двадцать девять стран-участник. Организация сама позиционирует себя как специальную площадку или форум, в ходе которого государства могут вести дискуссии, разрабатывать новые идеи для регулирования и усовершенствования социально-экономических направлений в мировой политике. В области информационных технологий важно упомянуть такую часть деятельности ОЭСР как рекомендации государствам-участникам по принятию или изменению новых законов и проектов.

Более поздним, но не менее важным видом источников международного права в сфере информационных технологий выступают решения и рекомендации органов и организаций международного уровня, в особенности, Совета Европы.

Одним из таким примеров является сентябрьское событие 1989 года. Именно тогда Совет Европы разработал Рекомендацию № R 89 (9) Комитета Министров стран-членов Совета Европы о преступлениях, связанных с

компьютером [83]. Некоторые эксперты [10], называют сентябрьскую Рекомендацию данного органа как достаточно неплохую, даже успешную попытку определения понятия компьютерных правонарушений и составления их перечня.

Рекомендация содержит в себе перечень главных принципов для национального права государств, согласно которым был определен и принят список действительных компьютерных преступлений, по поводу которых экспертным лицам удалось найти консенсус и подчеркнуть необходимость их криминализации в европейском уголовном праве. Более того, в Рекомендацию также включили описание и содержание тех пресечений закона, относительно которых не удалось достигнуть единого согласия, - иными словами, «факультативный перечень».

Данный документ не определил киберпреступления, но был разработан через составление порядка соответствующих действий и мер – такой подход вполне валиден, поскольку позволяет достаточно четко определить круг тех действий, что войдут в перечень «преступлений с использованием компьютера».

Основным документом Совета Европы по регулированию информационно-компьютерных технологий ученые по праву считают Конвенцию Совета Европы о преступности в сфере компьютерной информации ETS №185174 (Конвенция о киберпреступности)[31], разработкой которой занимался Комитет экспертов по преступности в киберпространстве, учрежденный Комитетом Министров Совета Европы в феврале 1997 года для изучения правовых проблем, появляющихся в ходе расследования преступлений с информационными технологиями. Конвенция сама по себе – универсальный акт, созданный для развития указанных в ней положений в национальном праве разных стран.

В сферу ее действия входят преступления в глобальных информационно-компьютерных пространствах, совершенные с помощью информационных

технологий. Конвенция содержит как нормы уголовного права о различных составах киберпреступлений, так и процессуальные – к примеру, процедуры во время расследования такого вида нарушений – выемка компьютерных данных и др.

Данный документ представляет собой важнейший международно-правовой акт в сфере кибербезопасности и регулирования расследования киберпреступлений, соответственно, имеет смысл рассматривать классификацию незаконных действий компьютерно-информационного характера именно с точки зрения этой Конвенции.

На региональном уровне также разрабатываются документы, регулирующие работы информационных технологий. Например, в рамках Содружества Независимых Государств (СНГ) проводится разработка специального списка главных принципов и условий привлечения к уголовной ответственности за преступную деятельность, осуществленную через или с помощью компьютерных технологий. По данному вопросу на постсоветском пространстве действует Межпарламентская Ассамблея государств-участников СНГ (МПА).

Ключевым в работе данного органа было седьмое пленарное заседание в феврале 1996 г., во время которого представители согласовали и приняли Модельный уголовный кодекс для стран-участников СНГ [33].

Что касается таких источников как доктрины, научные исследования юристов в международном праве, то, разумеется, они в достаточной мере влияют на развитие сферы международного права и безусловно могут быть применены в вопросах урегулирования отношений в области информационных технологий, но данный источник следует относить к вспомогательным.

Тем не менее, разрешение данного аспекта нельзя назвать достаточно эффективным в настоящее время, как полагают некоторые эксперты. К примеру, Ф. Кео [15], директор отдела информации информатики ЮНЕСКО, предполагает, что лучше создавать новые формы управления мировой

«инфоструктурой», потому что проблемы с распространением информационных технологий очень специфичны и существующие нормы и источники международного права крайне часто просто не могут их разрешить и устранить.

Иными словами, стоит уделять больше внимания вопросу о контролировании конкурентной борьбы между компаниями, предоставляющими услуги во Всемирной сети – ведь и здесь может возникнуть местный «гегемон», который захватит весь информационный рынок. Эксперт имеет в виду, что следует разработать международные антимонопольные законы в телекоммуникационной и других сферах, связанных с информационными технологиями. А также нужно создать программы тарифной политики и оказывать экономическую поддержку проектам по развитию телекоммуникаций на международном уровне.

Другие эксперты выдвигают идею о международном контроле Всемирной паутины специальными организациями, и при активном содействии мирового сообщества, такие органы могут возникнуть очень скоро, а также будут разработаны необходимые международно-правовые нормы для них.

Также популярна идея о создании центров информационно-технической поддержки странам, пострадавшим от последствий информационной войны, либо же крупной кибератаки, не говоря уже о разработке таких международных механизмов, которые смогли бы отслеживать информационные угрозы на постоянной основе для быстрого их предотвращения [86].

Сейчас мы можем говорить о том, что в документах отражены основные положения, касающиеся использования информационных технологий. Например, несанкционированные доступы к данным, их хищение, уничтожение и изменение. Также довольно глубоко проработаны вопросы, касающиеся преступлений с использованием компьютеров. Однако на данный момент все еще сложно регулировать отношения интеллектуальной собственности и информации. Остро стоят вопросы защиты информации, а также защиты прав

личности. До сих пор нет четкого ответа, кто несет ответственность за деяния автоматизированных информационных технологий.

В информационной сфере нормы международного права варьируются на широком диапазоне, а количество нормативно-правовых актов очень высоко, на данный момент не представляется возможность осуществить подробный анализ каждого из источников международного права, касающегося сферы информационных технологий, поэтому в будущем данная проблема будет разрешена, если удастся достичь консенсуса по поводу создания более универсального, масштабного документа, что охватывал бы большее количество аспектов регулирования информационно-технических областей.

2. Классификация и содержание киберпреступлений в международном праве

Прежде чем говорить о классификациях киберпреступлений, следует рассмотреть те виды правонарушений, что присутствуют в международном уголовном праве. Как правило, их делят на две группы – международные и транснациональные.

Международные преступления представляют собой действия особого опасного уровня, нарушающие ключевые принципы и нормы международного права [39]. Еще после событий Второй мировой войны, в 1945 г. в Уставе Международного военного трибунала [62] перечислили эти международные преступления – геноцид, военные пресечения закона, преступления против мира и человечности и т. д.

Вторая группа или транснациональные преступления – это те действия, которые не входят в список указанных выше деяний против человечества, но могут стать камнем преткновения в стабилизации международных отношений, расшатать мирное сотрудничество в различных сферах взаимодействия между странами и подставить под угрозу мирное сосуществование государств.

Преступления с информационными технологиями все еще не были внесены в перечень транснациональных преступлений по той причине, что в разных правовых системах стран юридические определения данных действий очень различаются. Официальное сообщение об этом было сделано представителями международного общества во время 10-го Конгресса Организации Объединенных Наций [14] по предупреждению преступности и обращению с правонарушителями. Они призывали сделать национальные законодательства государств едиными, унифицировать их.

Сотрудничество государств на международном уровне в области борьбы с киберпреступлениями можно улучшить, если согласовать определенные материальные нормы уголовного законодательства различных стран, а также

если в международном праве появится закрепленный перечень универсальных параметров оценки определенных действий как киберпреступлений. Конечно, для этого потребуются международно-правовые нормы, носящие обязательный характер в вопросе ратификации в национальном праве государств документов, привлекающих к уголовной ответственности за совершение правонарушений с информационными технологиями или частично с их помощью, ведь без этого такая составляющая регулирования на международно-правовом уровне как прецеденты международных судов просто не сможет существовать.

Как уже было указано в предыдущем разделе, в настоящее время ключевым нормативно-правовым актом международного уровня в сфере регулирования компьютерных преступлений является Конвенция о киберпреступности [31], имеет смысл обратиться к ее содержанию и классификации киберпреступлений. Также следует сказать о том, что данная Конвенция практически полностью покрывает весь спектр киберпреступлений и при рассмотрении других документов я буду сравнивать их с Конвенцией о киберпреступности.

Положения в документе относятся к следующим главным направлениями аспектов безопасности:

— сплочение и сближение маркеров и параметров уголовно-правового оценивания правонарушений, связанных с компьютерными данными;

— сближение направленных на поиск и сбор доказательств при расследовании компьютерных преступлений национальных уголовно-процессуальных процедур;

— развитие методов и форм международного взаимодействия и сотрудничество во время поиска и сбора доказательств совершения компьютерных преступлений заграницей в области уголовно-процессуальной деятельности.

Данный документ [31] предлагает странам-участницам закрепить в уголовном праве государств меры ответственности за преступления в сфере

информационных технологий. Он не сужает и не конкретизирует понятие «преступление в сфере компьютерной информации», но производит его замену на дефиницию «киберпреступление». Киберпреступления, в свою очередь, раскрываются через ряд деяний, которые входят в круг данного определения:

1) действия такого типа, которые посягают на компьютерные данные в преступном умысле, а также использующие эти данные как метод или инструмент в совершении правонарушения;

2) действия преступного характера, которые посягают на какие-либо охраняемые правом и законом блага и совершаются с помощью компьютеров или компьютерных данных.

Как изложено в Конвенции[31], объектом таких правонарушений выступает область общественных отношений, появляющихся в ходе реализации информационных процессов относительно сбора, хранения, передачи и других действий, осуществляемых с компьютерными данными, а также тех областей, в которых задействованы компьютерные технологии. Особую роль среди них носят те правовые отношения, что возникают в области конфиденциальности информационных систем и данных, законного применения информационных технологий и всего, что может касаться государственно важных сведений, либо же частной жизни граждан.

Были сформированы четыре группы общественно опасных действий в сфере компьютерной информации на основе следующих признаков:

1. Против конфиденциальности, целостности и доступности компьютерных данных и систем:

   — противоправный доступ;

   — перехват информации с помощью информационных технологий;

   — разрушение целостности содержания данных;

   —вторжение в системное функционирование компьютерных технологий;

   — использование ИКТ на противоправной основе.

2. Связанные с использованием компьютеров:

   — ввод, подмена, удаление или блокировка информации в компьютере;

   — мошенничество через использование компьютерной технологии для того, чтобы украсть собственность другого лица через ввод, подмену, стирание или блокировки компьютерных данных.

3. Связанные с содержанием данных:

   — деяния, связанные с порнографическими материалами с участием в них несовершеннолетних лиц.

4. Связанные с нарушением авторского права.

Субъектом вышеуказанных правонарушений выступает любое лицо, совершившее их.

Необходимо обратить внимание на тот факт, что ст. 12 Конвенции требует привлечения к ответственности институтов (организаций, международных в том числе) за преступные действия для получения выгоды юридическим лицом, совершенные сотрудником на руководящей позиции через превышение его полномочий. Уголовная ответственность юридического лица разрешается относительно той системы права, что закреплена в государстве-участнике [31].

Отдельно стоить отметить, что все киберпреступления, указанные в документе, могут быть поводом для привлечения к ответственности, только если были осуществлены умышлено. Помимо того, вместе с завершенными правонарушениями, Конвенция также призывает к привлечению к ответственности за покушение, соучастие или подстрекательство к совершению противоправного действия.

Можно сделать вывод, что данный документ достаточно подробно прорабатывает и указывает те аспекты, в рамках которых будут осуждены киберпреступники. Существует мнение, что некоторые органы, такие, как Министерство юстиции США, занимающееся в том числе расследованием

киберпреступлений, смогут расширить свои полномочия и включать практически любые средства для тестирования защитных программ в список «хакерских методов» [34].

В общем и целом, в Конвенции содержится практически полный перечень преступлений в киберпространстве, быть может, это все заслуга достаточно высокого уровня абстракции норм, но статьи документа в настоящее время захватывают почти максимально все те действия, что могут быть рассмотрены в качестве киберпреступлений.

Однако среди нормативно-правовых документов нельзя не упомянуть о Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» [13], подписанная в декабре 2003 года на Всемирной встрече на высшем уровне по вопросам информационного общества [11]. Двумя годами позже на этой же Встрече была подписана Тунисская программа для информационного общества от 2005 года [59].

Это две конференции под эгидой ООН, проведенные в Женеве (2003 г.) и Тунисе (2005 г.), в ходе которых были вынесены на обсуждение разносторонние аспекты применения потенциала информационных технологий для глобального социально-экономического развития, а также вопрос об управлении использованием и совершенствованием Интернет-сети.

В ходе Женевской Всемирной Встречи в 2003 г. были учреждены Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии»[13] и «Женевский план действий» [21]. Тунисская конференция 2005 г. знаменита за подписание таких нормативно-правовых актов, как «Тунисское обязательство» (WSIS-05/TUNIS/DOC/7-R) [59] и Тунисская Программа для информационного общества» (WSIS-05/TUNIS/DOC/6) [58].

Еще один документ Встречи, однако, носящий другой характер — Декларация «Формирование информационного общества в интересах человека»

[69]. Драйвером этой Декларации выступили гражданские предстваители Встречи.

Все документы имели схожесть в следующих пунктах:

— Каждый гражданин должен иметь свободный доступ к информации и информационным технологиям, для этого государствам необходимо повсеместно внедрять новые технологии;
— Основная повестка должна заключаться в вопросах регулирования Интернет-пространства, так как именно Интернет сейчас является общественным ресурсом информационного общества;
— При разработке документов, регулирующих Интрнет-пространствоб должны учувствовать все члены общества всех уровней, от государств и международных организаций до гражданских лиц.

В свою очередь интернет-сервисы были обозначены двух уровней. Первый уровень базового (например, адреса, протоколы и т. д. – все, что обеспечивает коммуникацию). Второй уровень с добавленной стоимостью (содержимое, электронные правительство и коммерция). Соответственно, обеспечить базовые сервисы — значит столкнуться только с технологическими проблемами, которые находятся в определенной зависимости от решений политиков, а вот уже чтобы применять и создавать сервисы второго типа, необходимо решать не только политические проблемы, но еще и социально-экономические, включая технологические аспекты.

Именно поэтому управление развитием и использованием сети (англ. Internet governance) как координирование работы заинтересованных лиц и институтов с разных сторон для обеспечения надежного и безопасного использования глобальной сети Интернет, носящей открытый доступ к собственным ресурсам представляет собой такой контроль за интернетом, который ведется путем разработки и использования правительствами и обществом граждан, которые выполняют не только собственную роль, но и

придерживаются общих принципов и правил, а также активно участвуют в программах и принятии решений, которые регулируют развитие и применение глобальной сети Интернет.

Документы, подписанные в ходе Встречи, также подчеркивают, как основные подходы следующие направления:

1) целостный подход к проблемам, имеющий не только технические, но и социально-экономические и политические характеристики;

2) толерантный и равноправный подход по отношению ко всем заинтересованным сторонам и лицам.

Что же касается идеи о глобальном информационном сообществе, то здесь свой вклад может сделать параграф 29 из Тунисской программы [58], в котором говорится, что регулирование использования Интернет-сети в международном масштабе должно быть разноплановым, прозрачным и демократичным, в котором примут участие правительства, организации и граждане, где будут обеспечены гарантии справедливого разделения ресурсов и где доступ будет облегченным для каждого желающего законного лица, несмотря на его расу, пол и другие характеристики. Очевидна все та же тенденция, которую продвигает международное сообщество, - толерантное отношение и свобода доступа для граждан любой культуры и социального положения.

Второй документ с данной Встречи, Тунисское обязательство[59], стал базисом для программ усовершенствования информационного сообщества разных государств, включая и государства из СНГ – к примеру, Республики Беларусь.

По итогам двух ВВУИО в период с 2003 по 2005 г.:

— организовали и учредили специальную рабочую группу по вопросам управления Интернетом (РГУИ)/Working Group on internet governance (WGIG) (2003–2005);

— приняли решение создать «фонд цифровой солидарности» для скорейшего устранения проблемы цифрового неравенства;

— узаконили право на коммуникацию в качестве позитивного, базового для реализации права на свободу слова и мнения;

— создали и опубликовали мандат – п. 72 в Тунисской программе [58] Форума по вопросам управления использованием интернета (ФУИ) (Internet governance forum IGF);

— сформировали требования, по которым в дальнейшем будут оценивать возможность возникновения угрозы от информационных технологий.

Также следует упомянуть, что Всемирная встречи в 2003–2005 гг. является одним из главных и первых примеров организации обсуждения такого уровня, в котором массово приняли участие представители гражданского сообщества.

В целом можно сказать, что Декларация 2003 года и Тунисская программа 2005 года сделали огромный шаг к построению нормативной базы регулирования информационных технологий и информационного общества. Был взять общий курс на защиту прав человека, расширение доступа к технологиям в развивающихся странах, продвижение цифровой экономики, однако, техническая часть вопроса, связанная с компьютерными технологиями затронута не была.

На региональном уровне тоже была проделана большая работа по регулированию информационных технологий . Совет Европы разработал ряд документов, регулирующих информационные технологии, а именно:

1. Конвенция «О взаимной правовой помощи по уголовным делам в том, что касается судебных поручений о перехвате телекоммуникационных сообщений» от 23 ноября 2001 года [29].

В данной конвенции основной упор сделан на преступления против целостности данных и компьютерной информации, а также на принципы международного сотрудничества. В данную Конвенцию не включили положения, которые бы предусматривали меру наказания за нарушения прав человека в информационном пространстве или интеллектуальной собственности.

2. Рекомендация Совета Европы «О борьбе с пиратством в области авторского права и смежных прав» от 5 сентября 2001 года [45].

В Рекомендации нет четкой классификации киберпреступлений, в документе правовые меры защиты и санкции разделены на 2 группы:

— уголовное право;

— гражданское право.

В данном контексте к уголовному праву мы относим те пиратские деяния, которые совершены юридическими и физическими лицами. И разработать нормативно-правовой акт, предусматривающий уголовное наказание, должны страны-участницы. К гражданскому праву, в большей степени, мы отнесем нарушение авторского и смешных прав, а работа над санкционными мерами проводится судом.

3. Конвенция «О защите физических лиц при автоматизированной обработке персональных данных» от 28 января 1981 года [30].

Название Конвенции говорит само за себя. Конвенция содержит основополагающие принципы защиты данных, а также процесс взаимопомощи между государствами при защите персональных данных. Однако данная Конвенция не содержит в себе четкой классификации преступлений и меры наказания.

4. Конвенция «По проблемам уголовно-процессуального права, связанным с информационными технологиями» [84].

Становится ясно из вышеприведённых Конвенций Совета Европы, что на данный момент нет единого документа, который бы полностью покрывал и классифицировал весь спектр киберпреступлений. Наиболее подробно была рассмотрела Конвенция Совета Европы «о киберпреступлениях». Можно сказать, что это единственная Конвенция, которая призывает стран-участниц привлекать к ответственности соучастников и подстрекателей преступления.

Еще один региональный документ действует в рамках СНГ. В 2001 году между десятью государствами-участниками СНГ было заключено «Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации» [54].

По Соглашению СНГ все преступления разделяются на несколько групп, а именно:

- создание, использование и распространение вредоносного программного обеспечения;
- получение неправомерного доступа к информации, если это повлекло изменение или уничтожение информации;
- нарушение регламента работы с ЭВМ, если это привело к уничтожению или блокировки охраняемой информации;
- незаконное использование данных, защищаемых авторским правом.

Как в Конвенциях, указанных выше, Соглашение в рамках СНГ не покрывает весь спектр киберпреступлений. Ничего не сказано о перехвате или дешифровании информации. Нет регламента работы в случаях несанкционированных атак со сторонних серверов и так далее. Можно сделать вывод о том, что Соглашение нуждается в дополнении с учетом появления новых видов информационного мошенничества и современных информационных технологий.

Исходя из анализа международных документов по вопросу устранения киберпреступности, мы видим, что странами подписаны несколько международных договоров. В общем и целом, те нормативно-правовые акты и национальные законы, которые существуют в настоящее время, сами по себе очень различны в плане содержания и степени охвата вопросов криминализации, следственных мер, международного сотрудничества и другое. Эти договоры, в свою очередь, могут быть как многосторонними, так и региональными, а также они очень различны в областях применения.

Именно все эти факторы становятся преградой для борьбы с киберпреступностью, ведь различия мешают быстро определять, расследовать и привлекать к ответственности преступных лиц в данной сфере, да и в принципе предупреждать все больше возрастающую угрозу киберпреступлений.

ГЛАВА III. Инициативы России по обеспечению информационной безопасности в современных международных отношениях

1. Деятельность России по обеспечению международной информационной безопасности в Организации Объединенных Наций

На современном этапе в российском законодательстве касательно информации содержится достаточно больше количество актов – более сорока федеральных законов, восьмидесяти актов Президента и приблизительно две сотни актов Правительства РФ. Но несмотря на все эти законодательные акты, отдельной киберстратегии как официального документа в России пока нет.

Если же рассматривать самые важные нормативно-правовые акты, то в первую очередь стоит обратиться к Доктрине информационной безопасности. Данный документ был выпущен в двух вариация – в 2000 г. [17], а затем в конце 2016 г [16]. В отличие от подхода Соединенных Штатов, Россия в собственном документе подчеркнула информационную безопасность сознания (индивидуального, группового, общественного) в качестве приоритетного направления.

Стоит упомянуть, что до 2000-х в Российской Федерации не было четко выражено отношение государства к информационной безопасности. Принятию данного документа поспособствовали события 90-х годов, в самом начале которых в государстве обеспечение информационной безопасности было катастрофически плохим. Либерально настроенные средства массовой информации выказывали отрицательное отношение и критику по отношению к безопасности, а отдельные специалисты заявляли, что во имя национальных интересов России стоит отказаться от принципа открытости и не участвовать в глобализации.

На выработку текста Доктрины ушло практически 10 лет. Их можно условно разделить на несколько этапов формирования документа.

1) Первый этап был связан с распадом СССР (1991-1996). На этом этапе в новом государстве — Российской Федерации были только основы законодательства, которые необходимо было дорабатывать и расширять. В этот период был принят Федеральный закон «Об информации, информатизации и защите информации» 20.02.1995 [64]. В это время Россию ждали успех в сотрудничестве с зарубежными странами, а также новая идентичность как игрока на международной арене и носителя интересов в информационной области. Как раз в этот момент и происходит вышеупомянутый спор между СМИ и экспертами, но большее количество лиц все склонялось к положительному сценарию, где Россия сможет стать участником мирового информационного пространства, причем не без оснований – РФ действительно делала много уступок, и необходимость защиты информационных ресурсов ставилась под вопрос. В информационной политике государства заимствовался западный опыт без должной адаптации, и эскалацией напряжения стали выборы Президента в 1996 г., в ходе которых противники устраняли друг друга через компрометирующую информацию, после чего чаша весов склонилась к другой стороне – необходимости защищать конституционный строй и духовную сферу. В последствии два этих направления стали частью первоначального текста документа [17]. Так как данный этап шел почти пять лет, то логичным его завершением стала замена тех правительственных деятелей, которые отвечали за информационную безопасность. Вдобавок России пришлось столкнуться с информационной войной из-за начавшихся в Чеченской Республике боевых действий, и в ней она терпела поражения.

2) Во время второго периода (1996–2000 гг.) в российском государстве уже начинают строиться и оформляться структуры и органы, отвечающие за вопросы информационной безопасности. Именно благодаря своевременной, последовательной и активной работе всех перечисленных выше правительственных органов первичный текст Доктрины был создан уже за первый год начала второго этапа – в 1997 г. [17]. Однако

внутригосударственные противоречия в правительстве, дефолт 1998 г. и другие обстоятельства извне так негативно повлияли на обстановку в стране, что сращу же принять документ не удалось. Это получилось сделать только три года спустя, к началу двадцать первого столетия.

Этот документ сам по себе – выражение официальные взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Тем не менее, информационная область не стояла на мести все эти года, а наоборот стремительно развивалась благодаря почти всем членам международной арены и ученым из самых разных государств – так, были созданы новейшие Web 2.0, а на их основе уже разработали и учредили социальные сети.

Отдельные из них существенно влияют на безопасность внутри государства – примером тому могут послужить события 2011 г в ближневосточном регионе [68]. Основное регулирование и координация этих явлений осуществлялось через известную социальную сеть «Twitter», за что они и получили название – «твиттер-революции».

Коснулось это не только Ближнего и Среднего Востока, но и постсоветского пространства – как могли наблюдать все жители Европы и европейской части Российской Федерации, в период с 2013 по 2014 г. в Украине тоже случилась цветная революция или же «Евромайдан» [20], как его принято называть. Регулирование этим процессом также происходило через «Twitter», поэтому его можно относить к тому же явлению, что и арабские протесты.

К слову, именно эти события перевернули российско-европейское и российско-американское сотрудничество, и именно после 2014 г. на Российскую Федерацию опустилось такое количество санкций, что это просто потребовало замены импортеров компьютерных технологий и переориентации на азиатские страны. Как современники данного процесса, многие

исследование имели возможность наблюдать это собственными глазами, в том числе читать официальные государственные источники, где говорилось о существенно возросшем уровне и мощи кибератак.

Тем не менее, не только негативные события произошли за эти года, но также и позитивные – расширилась законодательная база международного сообщества и Российской Федерации включительно, государства подписали новые документы по аспекту совершенствования компьютерных технологий. Поэтому становится очевидно, что старый текст Доктрины актуальной уже не характеризовался и потребовал изменений – Россия отреагировала на эту потребность в 2016 г. [16].

Что же касается участия во внешнеполитическом регулировании информационной сферы, то как и в любой другой области, Российская Федерация на пьедестал выносит именно главенствующую роль Организации Объединенных Наций – впервые информационной безопасности это коснулось в Концепции внешней политики РФ 2013 года [32].

Более того, следует обратить внимание на тот факт, что того, в «Основах государственной политики РФ в области международной информационной безопасности на период до 2020 г.» [36] Россия продолжает руководствоваться собственным интересом в приоритете ООН в системе международных отношений, так как отмечает одним из главных направлений противостоянию информационно-компьютерным угрозам всякое содействие созданию соответствующих документов именно в рамках этой организации, подчеркивая, что эти акты должны излагать основные принципы и нормы международного гуманитарного права в области информационно-компьютерных технологий.

Поскольку РФ последовательно подчеркивает нормативно-правовой контроль кибербезопасности на внутригосударственном уровне, то и на внешнеполитическом делает те же самые шаги – вопросы информационной безопасности требуют скорейшего урегулирования.

Не изменяя своим привычкам, Россия начиная с конца двадцатого века старается всеми силами утвердить собственные инициативы в ООН. Так, наше государство несколько лет назад создавало проект об учреждении специального международного трибунала по компьютерным преступлениям, но и здесь разделение сторон происходит именно по принципу «развитые-развивающиеся». Китай, Индия и Бразилия, партнеры России по множеству организации, с радостью ответили поддержкой на такое предложение, а запад и его восточные сторонники в очередной раз обратились к либеральным идеалам о бизнесе и заявили, что ограничение частного предпринимательства и свобод граждан в угоду информационной безопасности – это противоречие всем демократическим ценностям.

Однако нельзя не отметить, что далеко не всегда противостояние «запад-восток» происходит в полной мере, ведь иногда даже два полюса могут встретиться и найти общие концепты, в которых будут согласны. Такой компромисс, конечно, относительный, однажды случился зимой 2013 г. в Мюнхене, где проходила конференция по безопасности [56].

Здесь большинство стран наконец-то достигли консенсуса, что информационное пространство требует контроль именно со стороны международного-права, а не только в национальных законодательствах, ведь киберконфликты стали возрастать в масштабах. Несмотря на столько позитивное изменение, кардинальных мер принято не было. Была попытка российской-американской стороны, которая не увенчалась успехом. Стороны подготовили доклад, который могу бы послужить основой для выработки документа, регулирующего правила поведения при начале информационного конфликта. Однако он не повлиял на то, чтобы вынесенные решения не носили обязательный характер. Сам же доклад касался вопросов, в которых у двух сторон пока нет соглашений, но по которым они обязались вести дискуссию:

1) Распространяется ли запрет Женевского протокола на кибероружие.

2) Есть ли возможность законодательно и технически обособить защищенные объекты из массы незащищенных в информационном пространстве.

На конференции в Мюнхене стороны сделали еще одно попытку по регулированию информационного пространства. Предлагалось создать рамочную конвенции по вопросам информационных войн[87] и созвать международный трибунал по преступлениям в киберпространстве [87], где и будут решаться вышеобозначенные проблемы и вопросы.

В 1973 году было подписано Международное Телекоммуникационное Соглашение [19], а через три года в 1976 году Международное Соглашение о Морских Спутниках [43].

Согласно Соглашению 1973 года [19] и его тридцать пятой статье: все созданные и работающие станции не должны создавать помехи в работе коммуникационных сетей других государств. Исходя из этого утверждения можно сделал вывод, что статья Соглашения напрямую запрещает использовать спутниковые станции для вывода из строя коммуникационных сетей других стран. Также в Соглашении есть статья тридцать восемь, в которой говорится, что государства-члены могут создавать военные станции в рамках собственных армий, то есть, спутниковые системы тоже могут быть задействованы в военных операциях. А так как военная информация все равно проходит через гражданские системы, то между двумя положениями одного и того же документа встает противоречие.

В ходе диалогов по этой проблеме сформировались два подхода – западный и восточный.

Для США и других развитых страны главной целью является разработка мер информационной безопасности относительно преступных и террористических угроз, а такие опасные явления как информационные войны и оружие скорее описывал как нечто теоретическое, поэтому вопрос разоружения в проблеме международной информационной безопасности терял

свою актуальность в данном подходе. Дальнейший диалог по данному вопросу предлагали проводить по региональным форумам, а на базе ООН с акцентом на экономические и социально-культурные аспекты вопроса. Анализируя подход Америки становится понятно, что США не были заинтересованы в военном вопросе, говоря о том, что международному сообществу сначала нужен «практический» опыт в разрешения подобных конфликтов.

В свою очередь, РФ, КНР и развивающиеся государства придерживались идеи комплексного рассмотрения вопроса международной информационной безопасности. Главным направлением они определяли предупреждение угрозы информационной войны. Также, согласно их позиции, нужно в срочном порядке организовать обсуждение и практическую разработку основ международно-правового регулирования информационного пространства. Россия предложила создать специальный международный суд по киберпреступлениям.

Как подход США и развитых стран, так и подход России и развивающихся стран нашли отражение в Окинавской хартии 2000 года, однако, это добавило еще больше противоречий [35].

Во время пятьдесят третьей сессии ГА ООН Россия инициировала проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», консенсусом принятый в 1998 года [19]. Чуть позднее была принята Резолюция Генеральной Ассамблеи ООН A/RES/64/211 «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» [43].

В сентябре 2020 г. Владимир Владимирович Путин сделал официальное заявление - «О комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности (МИБ)» [37]. Глава Российской Федерации говорил о том, что мировому сообществу необходимо восстанавливать и активно учувствовать в

диалоге по обеспечению международной информационной безопасности. Владимир Путин сделал акцент на том, что только непрерывна работа международных площадок и бдительность государств позволит предотвратить инциденты безопасности как внутри отдельных государств, так и на всей международной арене.

В октябре 2020 г. Соединенные Штаты ответили на предложение России отказом [46]. Госсекретарь Майк Помпео сказал, что Россия разрушает целостность всемирной паутины, а все действия по регулированию информационного пространства являются бессмысленными [46]. Тем не менее, с приходом к власти администрации Джо Байдена, частично инициатива РФ была принята.

В июле 2021 г. была начата деятельность российско-американской рабочей группы по вопросам информационной безопасности [47], а тремя месяцами позже государства достигли договоренности об информации друг друга по поводу инцидентов в информационной среде.

Стоит упомянуть, что во время пленарного заседания ГА ООН в начале декабря 2021 года [42] была подписана российско-американская резолюция относительно мировой информационной безопасности, в которой впервые закрепили возможность разрабатывать юридические нормы обязательного характера в информационной сфере.

Однако в ходе последних событий после начавшейся на территории Украины специальной военной операции, в сотрудничестве с американской стороной и ООН в целом появились существенные трудности, поэтому 1 мая 2022 г. Президент РФ В. В. Путин подписал указ о дополнительных мерах кибербезопасности [60], но подчеркнул, что совместная деятельность с США и ООН на данный момент приостановлена из-за международно-политической обстановки.

Соответственно, можно сделать вывод, что в настоящий момент отсутствие универсального целостного законодательства в информационной

сфере является основной правовой проблемой. А имеющиеся соглашения противоречат друг другу. Например, в Международном Телекоммуникационном Соглашении [19], в ст.35 и в ст. 38 говорится о том, что на государства накладываются определенные запреты на столкновение или уничтожение спутниковых станций, но при этом государства сохраняют свободу действий при использовании их военных радиостанций.

Другим примером противоречий могут служить разные вгляды к обеспечению МИБ между странами. Так США делает акцент на террористических и преступных угрозах, а информационные войны ,например, считают чем-то теоретическим. С другой стороны Российская Федерация и развивающиеся государства предлагают разрабатывают комплексные меры и не акцентироваться-то только на одном аспекте.

Таким образом противоречия и разрозненность во мнениях стран приводит к тому, что двойственность международных Соглашений и Конвенций позволяет государствам истолковывать их в свою пользу.

2. Подходы России к обеспечению международной информационной безопасности в международных организациях и на межгосударственной основе

Россия, составляя собственную международную повестку дня относительно информационной безопасности мира в целом снова обращается к аспекту международно-правового контроля информационного пространства, а также включает туда проблемы правового управления информационными технологиями и др. Обосновывает Российская Федерация это тем, что поскольку количество и уровень опасностей в информационной области постоянно возрастает прямо во время разработки и создания правового режима международной информационной безопасности, то международному сообществу и институтам необходимо действовать кооперировано и слаженно.

Что касается же процесса формирования и совершенствования правовой основы, то это осуществлять необходимо постепенно, поэтапно — создание документов должно быть последовательным, чтобы они представляли собой единую систему. Все те нормативно-правовые акты, что носят глобальный характер, требуют детальной проработки, включая все договоренности, вынесенные в ходе проведения региональных форумов.

На современном этапе Российская Федерация вошла в большое количество соглашений по вопросам обеспечения массово-информационной безопасности (МИБ) на основе членства в таких организаций, как: Шанхайская Организация Сотрудничества (ШОС) [22], Организация Договора о коллективной безопасности (ОДКБ) [23], БРИКС [24], Содружество Независимых Государств (СНГ) [53]. Помимо этого, Россия также подписала перечень двусторонних соглашений по обеспечению МИБ с Республикой Беларусь [48], Китаем [49], Кубой [50], Индией[51] и Бразилией[52]. В данных актах указываются определения и формулировки угроз информационного

характера, и в большинстве своем они обозначены, как в национально-правовых российских документах.

Что касается межгосударственного сотрудничество, то здесь тоже было заключено несколько соглашений. Например, в 2016 году Россия и Индия подписали «Соглашение между правительством Российской Федерации и правительством Республики Индии о сотрудничестве в области обеспечения в сфере использования информационно-коммуникационных технологий» [51], в котором был сформирован перечень наиболее опасных и актуальных угроз, в число которых вошли:

— угроза использования информационных технологий во вред государственному суверенитету и национальных интересов;

— угроза несанкционированных атак по важнейшим структурам государственной информационной сети;

— угроза возникновения новой волны террористической пропаганды среди гражданского населения;

— угроза подрыва социального благосостояния с использованием информационных технологий.

Также следует упомянуть, что в сентябре того же года страны-участницы БРИКС встретились в Нью-Дели, чтобы обсудить предмет организации специальной экспертной группы по безопасности в информационном пространстве и противостоянию кибертерроризму.

Представители БРИКС сделали Совместное заявление, в рамках которого сообщили о достигнутых договоренностей. Страны договорились о совместных научных исследованиях, обмене опытом и совместных действиях по регулированию киберпространства. [24].

Между Россией и Китаем действует соглашение по вопросу обеспечения информационной безопасности на мировом уровне, заключенное в 2015 г. [49], в котором указывались понимания терминов и список угроз для МИБ.

Российское-китайское сотрудничество в этой сфере не заканчивается, потому что два государства в 2016 г. сделали официальное Совместное заявление. В нем они провозгласили, что охрана внутренних дел стран от угроз информационного вмешательства является приоритетом в их совместной деятельности. Россия и Китай также упомянули, что они и дальше собираются придерживаться принципа уважения суверенитета и культур друг друга в информационном пространстве, а любые действия, разжигающие ненависть, буду порицаемы и наказуемы.

Особенный акцент в Заявлении они сделали на том, что информационные технологии требуют совместных разработка, двустороннего обмена информаций и расширения сотрудничество в научно-технической сфере. В дополнение к Заявлению, были назначены ответственные лица за координирование работы органов власти в этой области. Со стороны России был назначен Игорь Олегович Щеголев, помощник Президента РФ. Китайское правительство выдвинуло на этот пост главу канцелярии Лу Вэя (Lu Wei).

Что касается более расширенного сотрудничества в рамках организаций, то было подписано Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения МИБ в 2009 году[22].

Таким образом, в перечне угроз можно обнаружить такие деяния, как:

— создание информационного оружия;

— международных терроризм с использованием информационных сетей;

— внешнее пагубное воздействие на общественную жизнь;

— установление контроля над каналами связи;

— использование сети Интернет для распространения запрещенной информации;

— киберпреступления;

— причинение умышленного ущерба с использованием информационных технологий;

— распространение информации, которая причиняет вред всем сферам политической и общественной жизни;

— угрозы безопасности техногенного характера.

Существует угроза распространения той информации, которая может вызывать беспорядки сразу в нескольких сферах жизни государств – например, общественно-политической и духовной, и согласно вышеуказанной классификации в этот список входит появление информации в Интернете, радио или телевизионной сфере, нарушающей представления о действительной политической системе, менталитете населения, а также пропагандирующей преступные действия, экстремизм и ненависть любого рода.

Данная угроза была адресована в ответ на те самые «твиттер-революции» или «Арабскую весну» [68] в ближневосточном регионе и цветную революцию в Киеве [20].

Данные соглашения, однако, больше затрагивают конфронтацию между государствами в информационной среде, но не берут в расчет негосударственных акторов. В большей части подписанных нормативно-правовых актов угрозой принято считать распространений той информации, которая является деструктивной для общественно-политической, духовной, культурной, нравственной, социально-экономической сфер общественной жизни государств, как уже было указано ранее, но кроме этих аспектов были выделены и другие. Например, использование социальных сетей как инструмент международных террористических организаций. Действительно с появлением социальных сетей наблюдается их рост и влияния не только общественную жизнь, но и на политическую обстановку. Существует еще такой проблемный аспект, что информация может не быть противоправной, и ее создателя к ответственности привлечь нельзя – тем не менее, это вовсе не отменяет ее вредоносности, что только усугубляет положение.

Так, видео с фейковой информацией сами по себе нарушением правового режима не являются на международном уровне, но большое количество таких

роликов приводит к тому, что это превращается в организованный процесс, оказывающий вредоносное влияние на людей. Соответственно, его можно приводить в качестве примера угрозы применения Интернет-сети в политических намерениях.

ЗАКЛЮЧЕНИЕ

Можно смело говорить о том, что влияние информационных технологий в последние десятилетия превзошли все ожидания. Сейчас речь идет не только об автоматизации политических процессов, но и глобальном пересмотре роли информационных технологий в международных отношениях.

В ходе анализа источников и написания работы я рассмотрела и выполнила все поставленные задачи, а также достигла главной цели: детально изучены теоретические и практические основы, а также влияние информационных технологий на международные отношения. Определены основные документы, регулирующие информационные технологии на мировой арене.

Подводя итоги, можно бесспорно утверждать, что информационные технологии развиваются с каждым годом, а рост влияния на международные отношения растет с геометрической прогрессией. Сейчас информационные технологии способны заменить часть процессов, которые ранее выполнялись человеком. Об этом нам открыто сообщает электронное правительство. Однако нормативно-правовое регулирование все еще не так детально проработано, как требует ситуация. В международном праве все еще стоит вопрос о защите персональных данных, интеллектуальной собственности, а также вопрос об ответственности за созданные и использование информационных технологии. Можно сказать, что логичны были бы дальнейшие шаги по развитию и дополнению Конвенции Совета Европы о киберпреступлениях, однако, как мы видим, последние Рекомендации и Конвенции принимаются для узкого круга проблем.

Что касается международного сотрудничества, то здесь заключаются соглашения и создаются конвенции как на глобальном, так и на региональном уровне. Отдельное место в этом иерархии занимают соглашения между государствами. На данный момент самый ожидаемый вариант сотрудничества

России по обеспечению международной информационной безопасности будет со странами ШОС и СНГ. Как показала история, через ООН Россия и ее инициативы по обеспечению МИБ терпели неудачи, логично, что было принято решение обратить внимание членов ШОС на данные вопросы. С 2011 г. КНР и Республика Казахстан выбрали ту же стратегию – использование площадки Организации для регулирования информационного пространства. В 2014 г. Россия вынесла информационную безопасность в приоритетные задачи повестки дня в организации.

В качестве еще одной площадки для продвижения инициатив, Российская Федерация обратила внимание БРИКС. В рамках организации сотрудничество по вопросам МИБ является одним из приоритетных направлений. Также на повестке «Центр киберугроз БРИКС», который должен предупреждать киберпреступления, как уже делают РФ и США.

Подводя итоги можно говорить о том, что информационные технологии опережают само время. Быстрый темп развития не позволяет международным организациям оперативно принимать и обновлять документы, которые регулировали бы информационные технологии. При этом межрегиональное и межгосударственное сотрудничество не стоит на месте, с каждым годом все больше стран проявляют инициативы по обеспечению международной информационной безопасности и развитию информационных технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алексеева И. Ю. Развитие информационного общества в России / И. Ю. Алексеева. — Москва : ИФ РАН, 2016. — 196 с.
2. Артюх А. А. Киберпространство: лучший выход — это вход / А. А. Артюх // Искусство кино. — 2004. — № 4. — С. 31-39.
3. Бауэр, Ф. Информатика. Вводный курс / Ф. Бауэр, Г. Гооз. — Москва : Мир, 1990. — 366 с.
4. Большой энциклопедический словарь / ред. А.М. Прохоров. — Москва : Советская Энциклопедия, 1991. — 941 с.
5. Бюллетень международных договоров [Электронный ресурс] // Официальный сайт собрание законодательства Российской Федерации. — Режим доступа: https://www.szrf.ru/szrf/docslist.php?md=0&nb=102&year=&issid=1022002011000&div_id=2, — свободный.
6. Василенко Л. А. Интернет в информатизации государственной службы России / Л. А. Василенко. — Москва : РАГС, 2000. — 252 с.
7. Ведомости [Электронный ресурс] // Официальный сайт российской академии наук. — Режим доступа: http://www.ras.ru/digest/showdnews.aspx?id=97c1a6ce-dd9a-41b2-b903-efb92addaad7, — свободный.
8. Венская конвенция о праве международных договор от 23.05.1969 [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/law_treaties.shtml, — свободный.
9. Винер, Н. Кибернетика и общество / Н. Винер. — Москва : АСТ, 2019. — 288 с.

10. Волеводз А.Г. Правовые основы новых направлений международного сотрудничества в сфере уголовного процесса: дис. д-р. юр. наук: 12.00.09. — Москва, 2002. — 462 с.
11. Всемирная встреча на высшем уровне по вопросам информационного общества [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://www.un.org/ru/events/pastevents/wsis.shtml, — свободный.
12. Дезинформация в промышленных масштабах. Мониторинг организованных манипуляций в социальных сетях 2020 [Электронный ресурс] // Научно-технический центр ФГУП ГРЦЧ. — Режим доступа: https://rdc.grfc.ru/2021/09/industrialized-disinformation-2020-global-inventory-of-organized-social-media-manipulation, — свободный.
13. Декларация принципов построение информационного общества – глобальная задача в новом тысячелетии от 12.12.2003 [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf, — свободный.
14. Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями /Документ ООН A/CO№M87/Ю.
15. Дипломатический вестник. — 2000. — №8. — С. 51-56.
16. Доктрина информационной безопасности Российской Федерации от 05.12.2016 [Электронный ресурс] // Официальный сайт ГАРАНТ.РУ. — Режим доступа: https://clck.ru/hcqXN, — свободный.
17. Доктрина информационной безопасности Российской Федерации от 09.09.2000 [Электронный ресурс] // Официальный сайт ГАРАНТ.РУ. — Режим доступа: https://base.garant.ru/182535/, — свободный.
18. Долгов С. И. Глобализация экономики: новое слово или новое явление / С. И. Долгов. — Москва : Экономика, 1998. – 213 с.
19. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://clck.ru/NFLfn, — свободный.

20. Евромайдан: как все начиналось [Электронный ресурс] // Официальный сайт BBC — Режим доступа: https://www.bbc.com/ukrainian/features-russian-42065355, — свободный.
21. Женевский план действий от 12.12.2003 [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://www.un.org/ru/events/pastevents/pdf/plan_wsis.pdf, — свободный.
22. Заседание группы экспертов государств-членов ШОС по международной информационной безопасности от 12.11.2019 [Электронный ресурс] // Официальный сайт ШОС. — Режим доступа: http://rus.sectsco.org/news/20191112/599223.html, — свободный.
23. Заявление министров иностранных дел государств – членов Организации Договора о коллективной безопасности о совместных мерах по обеспечению информационной безопасности от 17.07.2017 [Электронный ресурс] // Официальный сайт ОДКБ. — Режим доступа: https://odkb-csto.org/documents/documents/zyavlenie_ministrov_inostrannykh_del_gosudarstv_chlenov_organizatsii_dogovora_o_kollektivnoy_bezopas/#loaded, — свободный.
24. Заявление стран БРИКС по подготовке соглашения в информационной безопасности [Электронный ресурс] // Официальный сайт РИА. — Режим доступа: https://ria.ru/20180629/1523671244.html, — свободный.
25. Комиссия по информационной безопасности [Электронный ресурс] // Официальный сайт Регионального содружества в области связи. — Режим доступа: https://www.rcc.org.ru/o-rss/arhiv/komissiya-po-informatsionnoy-bezopasnosti/, — свободный.
26. Конвенция о защите физических лиц при автоматизированной обработке персональных данных ETS № 108 [Электронный ресурс] // Консультант Плюс. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121499/, — свободный.

27. Конвенция ООН по торговле и развитию от 30.12.1964 [Электронный ресурс] // Официальный сайт ЮНКТАД. — Режим доступа: https://www.un.org/ru/ga/unctad/, — свободный.
28. Конвенция ООН по торговле и развитию от 30.12.1964 [Электронный ресурс] // Официальный сайт ЮНКТАД. — Режим доступа: https://www.un.org/ru/ga/unctad/, — свободный.
29. Конвенция Совета Европы «О взаимной правовой помощи по уголовным делам в том, что касается судебных поручений о перехвате телекоммуникационных сообщений» от 23.11.2001 [Электронный ресурс] // Официальный сайт ГАРАНТ.РУ. — Режим доступа: https://base.garant.ru/4089723/, — свободный.
30. Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» от 28.01.1981 [Электронный ресурс] // Официальный сайт Консультант Плюс. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121499/, — свободный.
31. Конвенция Совета Европы о преступности в сфере компьютерной информации от 23.11.2001 [Электронный ресурс] // Официальный сайт ГАРАНТ.РУ. — Режим доступа: https://base.garant.ru/4089723/, — свободный.
32. Концепция внешней политики Российской Федерации от 12.02.2013 [Электронный ресурс] // Официальный сайт ЗКНПА. — Режим доступа: https://legalacts.ru/doc/kontseptsija-vneshnei-politiki-rossiiskoi-federatsii-utv-prezidentom/, — свободный.
33. Модельный Уголовный Кодекс для государств – участников Содружества Независимых Государств от 17.02.1996 [Электронный ресурс] // Официальный сайт МККК. — Режим доступа: https://www.icrc.org/ru/doc/resources/documents/misc/ihl-nat-3.htm, — свободный.

34. Обращение общественных организаций с протестом против принятия Конвенции о киберпреступности // Бизнес-разведка и информационный менеджемнт. — 2002. — №6.
35. Окинавская хартия глобального информационного общества от 21.07.2000 [Электронный ресурс] // Официальные сетевые ресурсы президента России. — Режим доступа: http://www.kremlin.ru/supplement/3170, — свободный.
36. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года от 24.07.2013 [Электронный ресурс] // Консультант Плюс. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_178634/, — свободный.
37. Официальное заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности» от 25.09.2020 [Электронный ресурс] // Официальный сайт Международная жизнь. — Режим доступа: https://interaffairs.ru/news/show/27573, — свободный.
38. Панарин И. Н. Информационное общество и геополитика / И. Н. Панарин. — Москва : Поколение, 2006. — 560 с.
39. Панов В.П. Международное уголовное право / В.П. Панов. — Москва: Инфра-М, 1997.— 320 с.
40. Поверинов И. Е. Информационное пространство социума: структура, трансформация и региональная специфика / И. Е. Поверинов. — Саранск : Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва, 2005. — 188 с.
41. Проблемы преступности в капиталистических странах. — 1987. — № 9. — С. 19.

42. Резолюции 76-й сессии 2021-2022 ООН [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://www.un.org/ru/ga/76/docs/76res3.shtml, — свободный.
43. Резолюция Генеральной Ассамблеи ООН A/RES/64/211 Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур от 21.11.2009 [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement, — свободный.
44. Рейнгольд Г. Г. Умная толпа: новая социальная революция / Г. Г. Рейнгольд. — Москва : Фаир-Пресс, 2006. — 416 с.
45. Рекомендация Совета Европы «О борьбе с пиратством в области авторского права и смежных прав» от 05.09.2001 [Электронный ресурс] // Официальный сайт Кодекс. — Режим доступа: https://docs.cntd.ru/document/90199651,— свободный.
46. Речь Майка Помпео от 20.10.2020 [Электронный ресурс] // Официальный сайт Бизнес онлайн. — Режим доступа: http://www.business-gazeta.ru/news/485178, — свободный.
47. Россия и США налаживают сотрудничество в сфере информационной безопасности [Электронный ресурс] // Официальный сайт РСМД. — Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/rossiya-i-ssha-nalazhivayut-sotrudnichestvo-v-sfere-informatsionnoy-bezopasnosti/8, — свободный.
48. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25.12.2013 [Электронный ресурс] // Официальный интернет-портал

правовой информации. — Режим доступа: http://docs.cntd.ru/document/499074140, — свободный.

49. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 08.05.2015 [Электронный ресурс] // Официальный интернет-портал правовой информации. — Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1, — свободный.
50. Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности от 10.07.2014 [Электронный ресурс] // Официальный интернет-портал правовой информации. — Режим доступа: http://ips.pravo.gov.ru/?docbody=&link_id=41&nd=102355279&intelsearch=, — свободный.
51. Соглашение между правительством Российской Федерации и правительством Республики Индии о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий от 15.10.2016 [Электронный ресурс] // DRUSSIA. — Режим доступа: https://d-russia.ru/wp-content/uploads/2017/01/Russia_India_IKT.pdf, — свободный.
52. Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности от 13.05.2010 [Электронный ресурс] // КонсультантПлюс. — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=480062#06299361257489029, — свободный.

53. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 [Электронный ресурс] // Официальный сайт Кодекс. — Режим доступа: https://docs.cntd.ru/document/902140948,— свободный.
54. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 [Электронный ресурс] // Официальный сайт Кодекс. — Режим доступа: https://docs.cntd.ru/document/902140948,— свободный.
55. Солдатов С. Желтые страницы Internet / С. Солдатов. — Санкт-Петербург : Питер, 1998. — 600 с.
56. Сорок девятая Мюнхенская конференция по безопасности 01.02.2013 – 03.02.2013
57. Торкунов А. В. Современные международные отношения и мировая политика / А. В. Торкунов. — Москва : Просвещение, 2004. — 992 с.
58. Тунисская программа для информационного общества от 15.11.2005 [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf, — свободный.
59. Тунисское обязательство от 18.11.2005 [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://www.lawtrend.org/wp-content/uploads/2014/07/TUNISSKOE-OBYAZATELSTVO.pdf, — свободный.
60. Указ о дополнительных мерах по обеспечению информационной безопасности Российской Федерации от 01.05.2022 [Электронный ресурс] // Официальный сайт Президента России. — Режим доступа: http://kremlin.ru/acts/news/68322l, — свободный.

61. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательство РФ. — 2016. — № 50.
62. Устав Международного Военное Трибунала для суда и наказания военных преступников от 08.08.1945 [Электронный ресурс] // Официальный сайт Консорциум кодекс. — Режим доступа: https://docs.cntd.ru/document/901737883, — свободный.
63. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [Электронный ресурс] // Консультант Плюс. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, — свободный.
64. Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» [Электронный ресурс] // Консультант Плюс. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5887/, — свободный.
65. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // Консультант Плюс. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/84d089988c5c4a7c2e9021c6f46b85a00cd641c3/, — свободный.
66. Федеральный закон РФ от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Консультант Плюс. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, — свободный.
67. Федерльный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // Консультант Плюс. — Режим доступа: https://studresearsh.ru/4oformlenieIstochnikov/4_9_kakOformitVspiskeLiteraturiFederZakon.html#:~:text=%D0%9E%D1%84%D0%BE%D1%80%D0%BC

%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D1%84%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85%20%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%BE%D0%B2%20%D0%B2%20%D1%81%D0%BF%D0%B8%D1%81%D0%BA%D0%B5,%E2%80%93%202011, — свободный.

68. Фитуни Л. Арабская весна: трансформация политических парадигм в контексте международных отношений // Мировая экономика и международные отношения. —2012. — №1. — с. 3-14.
69. Формирование информационных обществ в интересах человека от 08.12.2003 [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://www.itu.int/net/wsis/docs/geneva/civil-society-declaration-ru.pdf, — свободный.
70. Цыганков П. А. Теория международных отношений / П. А. Цыганков. — Москва : Гардарики, 2007. — 993 с.
71. Цыганков П.А. Глобальные политические тенденции и социология международных отношений / П. А. Цыганков. — Москва, 1998. — 240 с.
72. Чесноков А.А. Ресурсы INTERNET и российские политические технологии: состояние и перспективы развития // Вестник МГУ. - 1999. - №4. – С. 24-33.
73. Шеннон, К. Работы по теории информации и кибернетики / К. Шеннон. — Москва : Букинистика, 1963. — 830 с.
74. Шипилов А. И. Инстинкт территории / А. И. Шипилов // Компьютерра. — 1998. — № 2. — С. 7-13.
75. ЮНЕСКО Между двумя этапами Всемирного саммита по информационному обществу. — Санкт-Петербург, 2005. — 451 с.
76. Darrel M. Jurisdiction In Cyberspace: A Theory of International Spaces / M. Darrel // Michigan Telecommunications and Technology Law Review. — 1998. — №4. — С. 3-36.

77. Davis R. The Web of Politics: The Internet's Impact on the American Political System / R. Davis. — NY : Oxford University Press, 1999. — 248 p.
78. Dijk J. Virtual democracy: Issues of theory and practice / J. Dijk. — NY: SAGE Publications Ltd, 2001. — 240 p.
79. Glassman J. K. Glassman Public Diplomacy 2.0: A New Approach to Global Engagement [Электронный ресурс] // Washington, DC: 2008. — Режим доступа: https://2001-2009.state.gov/r/us/2008/112605.htm — свободный.
80. Hacker K. Internet and Democracy in the Network Society/ K. Hacker. — London : Routledge, 2018. — 218 p.
81. O'Neill K. Pixels and Place: Connecting Human Experience Across Physical and Digital Spaces / K. O'Neill. — London : KO Insights, 2016. — 224.
82. Recommendation № R 87 (18) of the Committee of Ministers of the Council of Europe. — 1987.
83. Recommendation № R 89 (9) of the Commitee of Ministers of the Council of Europe to member States for the Computer-Related Crime and Final Report of the European Commitee on Crime Problems. — Strasbourg, 1990.
84. Recommendation № R 95 (13) of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology. — Strasbourg, 1995.
85. RU-CERT [Электронный ресурс] // Центр реагирования на компьютерные инциденты. — Режим доступа: https://www.cert.ru/ru/about.shtml, — свободный.
86. The Clinton Gore Administration: From Global Digital Divide to Digital Opportunity [Электронный ресурс] // President Clinton and Other G-8 Leaders: 2000. —
Режим доступа:http://www.ecommerce.gov/ecomnews/pr0725002.html, — свободный.
87. The Third Pillar for Cyberspace An International Court or Tribunal for Cyberspace [Электронный ресурс] // Официальный сайт CyberCrime Law.

— Режим доступа: https://www.cybercrimelaw.net/documents/Draft_Treaty_text_on_International_Criminal_Tribunal_for_Cyberspace.pdf, — свободный.

88. Westcott, N. Digital Diplomacy: The Impact of the Internet on International Relations / N. Westcott. — Oxford Internet Institute, 2008. — 20 p.
89. World Resources Institute [Электронный ресурс] // Официальный сайт Института мировых ресурсов. — Режим доступа: http ://www.wri.org, — свободный.

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 технологии в современных международных отношениях

Руководитель Мороз 24.05.22 профессор, д.и.н Е.В. Мороз
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник 24.05.2022 Ю.В. Пьянкова
подпись, дата инициалы, фамилия

Красноярск 2022