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
« ___» _____ 2023 г.

# БАКАЛАВРСКАЯ РАБОТА

41.03.05. Международные отношения

Роль международных организаций в обеспечении информационной безопасности государств

| | | | |
|---|---|---|---|
| Руководитель | _____<br>подпись, дата | доцент, к.ю.н<br>должность, ученая степень | В.А. Мещериков<br>инициалы, фамилия |
| Выпускник | _____<br>подпись, дата | | А.А. Пахомчик<br>инициалы, фамилия |

Красноярск 2023

# СОДЕРЖАНИЕ

# Введение

**Актуальность темы исследования.** Появление компьютеров и Интернета произвело беспрецедентную революцию в человеческой цивилизации. Хотя киберпространство значительно облегчает жизнь по многим параметрам, эра информационных технологий, но и, к сожалению, послужило появлению новых составов преступлению в информационной сфере. Данное обстоятельство осложнило борьбу с преступностью в киберпространстве. Сегодня почти все государственные и частные учреждения, а также население, зависят от компьютерных систем и сетей для хранения конфиденциальной информации, потеря которой может привести к необратимым последствиям и значительному ущербу, что требует срочных глобальных действий по борьбе с киберпреступностью.

Киберпреступность определяется как любое «действие, нарушающее закон, которое совершается с использованием информационных и коммуникационных технологий (ИКТ), направленное либо на сети, системы, данные, веб-сайты и/или технологий или для содействия преступлению» [37]. Примеры киберпреступлений включают в себя хакерство, незаконный перехват телекоммуникаций, киберпреследование, кража личных данных, введение в заблуждение и т.д. Они представляют серьезную угрозу для конфиденциальности, целостности, безопасности и доступности критически важной компьютерной инфраструктуры, что может привести к сбоям в работе, финансовым потерям, ущербу репутации, потере интеллектуальной собственности и неоправданным расходам.

В настоящее время международная деятельность по защите информации является, несомненно, важной и необходимой по многим причинам. Увеличение объемов ценной информации, рост числа киберпреступлений, повышение уровня осведомленности общественности о киберугрозах, рост информационных технологий в экономике и социальной сфере, и наконец – политическая ситуация внутри и вне государств. Современные государства, в

связи с глобальной цифровизацией, переходит в режим повышенной бдительности и, в частности, старается всеми силами противостоять и киберпреступности. Из-за быстрого роста технологий, необходимость в защите как личной, так и государственной информации, является предметом обсуждения международных организаций.

**Степень научной разработанности.** Прежде всего, стоит выделить работы Жаглина А.В [23], Ирошникова Д.В [27], Татузова А.Л. и Безкоровайного М.М [16], в которых рассматриваются вопросы терминологии информационной безопасности и кибербезопасности. Научно-исследовательскую основу проблемам международного сотрудничества в области обеспечения международной кибербезопасности составляют работы следующих авторов: Касеновой М. Б [32], Кардавы Н.В [31], Капустина А. Я. [30].

Современные информационные технологии часто становятся источником киберугроз и киберопасностей, для анализа новейших информационных технологий в данной работе использованы работы Душкина Р.В [22], Потапова А.С [51], Мурзина Ф.А. [47], Калашникова А.О., Аникиной Е.В [29], Запечникова С.В [25], Цветкова В.Я [53].

**Объектом работы** является международные отношения между государствами в обеспечении информационной безопасности государств.

**Предмет работы** – исследовать место и значение международных организаций в обеспечении информационной безопасности государств.

**Целью исследования** - анализ роли международных организаций в обеспечении информационной безопасности государств.

Поставленная цель обуславливает **решение следующих задач:**

Изучить систему международной информационной безопасности в современном мире;

Рассмотреть политику ООН в области обеспечения международной информационной безопасности;

Проанализировать значение БРИКС, ШОС и ОДКБ в осуществлении мировой безопасности в информационном пространстве;

Сравнить универсальный и региональный подходы в области обеспечения международной информационной безопасности.

**Теоретическая и практическая значимость исследования** заключается в том, что это комплексное исследование кибербезопасности в системе международных организаций и роли, и значения этих организаций для развития международной кибербезопасности. Результаты исследования могут быть использованы при преподавании курсов по международным отношениям, правоохранительной деятельности, а также при создании учебников по указанным дисциплинам.

Структура работы: поставленные цель и задачи определяют структуру всей работы. Она состоит из введения, двух глав, заключения и списка литературы.

# 1 Цифровая повестка в контексте мировой безопасности

## 1.1 Теоретические аспекты международной информационной безопасности

Сегодня сфера международной и национальной безопасности является одной из ключевых отраслей деятельности любого государства, предметом внутриполитической борьбы, внимания гражданского общества, научных исследований. Это, в свою очередь, требует обдуманного подхода к проблемам национальной и международной безопасности со стороны не только специалистов, но и наиболее широкого круга граждан. Благодаря этому, проблемы национальной и международной безопасности стали частью образовательной программы университетов.

В современном мире активно развивается новая область знаний для решения проблем безопасности в сфере ИКТ. Кибербезопасность и информационная безопасность сегодня являются общепринятыми терминами. Эти термины обычно используются как взаимозаменяемые.

На основании стандарта ISO/IEC 27032:2012, кибербезопасность определяется как «сохранение конфиденциальности, целостности и доступности информации в киберпространстве», информационная безопасность, с другой стороны, определяется как «сохранение конфиденциальности, целостности и доступности информации» [59]. Основной целью информационной безопасности является обеспечение непрерывности различных процессов с наименьшим ущербом и ограничение негативных последствий различных инцидентов.

Таблица 1 – определения Информационной и Кибербезопасности

| **Информационная безопасность** | **Кибербезопасность** |
|---|---|
| Информационная безопасность рассматривает безопасность компьютерных систем для защиты их от раскрытия, субъективной модификации, | Кибербезопасность рассматривает безопасность отдельных лиц и предприятий с целью защиты их от нарушений безопасности, инцидентов и |

| | |
|---|---|
| несанкционированного доступа | преднамеренных атак на системы |
| Информационная безопасность включает в себя защиту информации от различных угроз, направленных на минимизацию риска деловой активности, максимизацию возврата инвестиций, использования возможностей бизнеса и обеспечения непрерывность бизнеса. Соображения информационной безопасности направлены на целостность, конфиденциальность и доступность информационных ресурсов | Сфера кибербезопасности распространяется на защиту информации и ИКТ, включая поддержание целостности, конфиденциальности и доступности информационных ресурсов в киберпространстве. Кибербезопасность включает защиту инструментов, систем, процессов, концепции, методы и стратегии, направленные на защиту имущества в киберпространстве от несанкционированного доступа и потери информации что приводит к сохранению целостности, конфиденциальности и доступности ресурсов |
| Информационная безопасность рассматривает целостность, конфиденциальность и доступность информации независимо от типа данных, будь то печатные или электронные | Кибербезопасность относится к мерам, которые принимаются для обеспечения дружественного использования компьютерных систем и предотвращения несанкционированной эксплуатации информация |
| Информационная безопасность определяется как "защита информации и ее критических элементов, включая системы и аппаратные средства, которые используют, хранят и передают эту информацию" | Совокупность политик, инструментов, руководств, концепций, подходов, мер, технологий, передовой практики и обучения, которые используются для сохранения кибер-активов организации и пользователей, признается как кибербезопасность |
| Использование логического и физического контроля доступа для обеспечения безопасности данных и предотвращения несанкционированного доступа к данным, потери данных, неправомерное использование данных, повреждение, раскрытие или уничтожение данных | Совокупность процессов, инструментов, структур и ресурсов, которые используется для защиты систем в киберпространстве, признается как кибербезопасность |

Принимая во внимание определения, представленные в таблице, можно сделать вывод, что информационная безопасность полностью включает в себя кибербезопасность как один из своих компонентов. Кибербезопасность, с другой стороны, отвечает за обеспечение безопасности информации от киберугроз и кибератак во время ее обработки, хранения или транспортировки.

Контроль доступа, процедурный контроль, контроль соответствия и технический контроль являются примерами информационной безопасности, в то время как безопасность приложений, сетевая безопасность, облачная безопасность и критическая инфраструктура являются примерами кибербезопасности.

Компьютеризация и информационная революция открыли путь научно-технической революции во многих отраслях. Все больше становится разрыв между передовыми в технологическом плане странами и другим миром. Такое положение дел объективно стимулирует отсталые в научно-технологическом отношении страны или присоединяться к коалициям высокоразвитых стран [16].

Информация приобрела системообразующее значение во всех сферах жизнедеятельности, с другой - информационная инфраструктура приобретает статус критической (жизненно важной для существования государства) и требует для своей защиты сбалансированной государственной политики, в частности в информационной сфере. Стремительное развитие информационно-коммуникационных технологий (ИКТ) способствует налаживанию широкого международного сотрудничества. Однако отдельные достижения в информационной сфере могут использоваться в целях, противоречащих поддержке международной безопасности и стратегической стабильности. Растут масштабы киберпреступности и кибертерроризма. Особую озабоченность вызывает возможность применения информационно телекоммуникационных технологий для подготовки и осуществления террористических актов в мире [54].

В современных условиях информационная безопасность становится органическим элементом национальной безопасности, поскольку информация превращается в ресурс не только национального стратегического, но и мирового значения. Соответственно при разработке концепций, стратегий, целевых программ и планов действий по обеспечению национальной безопасности государства следует учитывать изменения в пространстве угроз и

вызовов, обусловленные расширением влияния информационного фактора в условиях глобализации.

Информационная безопасность – это статус защиты систем обработки и хранения данных, который обеспечивает конфиденциальность, доступность и целостность информации, для ее использования в интересах граждан. Информационная безопасность характеризуется степенью защиты и стабильности основных сфер жизни, а также информационным воздействиям как к внедрению, так и к изъятию информации. Понятие информационной безопасности не ограничивается безопасностью технических информационных систем или защитой информации в цифровой или электронной форме, но также применяется ко всем аспектам защиты данных или информации, независимо от их формы.

Информационная безопасность – это не только защита информации от несанкционированного доступа. Информационная безопасность – это в основном практика предотвращения несанкционированного доступа, использования, разглашения, срыва, изменения, модификации, проверки, записи или уничтожения информации. Информация может быть физической или электронной.

Информационное общество – это общество, которое преимущественно обрабатывает информацию на основе использования информационно-коммуникационных технологий. Информационными ресурсами могут пользоваться все слои населения. Это показывает, что при формировании информационного общества и электронного управления все вещи, связанные с этой концепцией, являются актуальными. Информационная безопасность рассматривается как состояние защищенности объектов от информационных угроз), которое может предотвращать негативные информационные воздействия и негативные последствия информационных технологий или специальных информационных операций, внешней информационной агрессии и секретного удаления информации (с помощью специального технического метода).

Анализ различных методов определения содержания концепции информационной безопасности позволяет заметить неудобство избрания позиции. Сегодня этот вопрос необходимо рассматривать комплексно и систематически. Самым приемлемым является комплексный подход, при котором информационная безопасность будет определяться путем изложения ее важнейших характеристик, с учетом постоянных изменений информационных систем и формирования незащищенности. Реализация информационной безопасности может рассматриваться не только как потребность страны, но и как потребность других субъектов информационных отношений: граждан, юридических лиц, технических механизмов, систем, информационно-коммуникационных технологий, объектов информационной безопасности.

Информационная безопасность также рассматривается как состояние информационной безопасности (защита объекта от информационных угроз), которое может предотвратить негативное влияние информации и операции вторжения информационных технологий и секретного извлечения информации (с помощью специальных технических средств). Информационный терроризм и компьютерные преступления наносят значительный ущерб национальным интересам страны и не влияют на стабильное развитие информационной инфраструктуры и нормальную работу национального информационного пространства.

Учитывая глобальный характер информационной безопасности, развитые государства начали реализовывать долгосрочные программы, направленные на защиту ценных информационных структур.

Стратегия глобального противостояния информации является основой для анализа и развития исследовательских учреждений в разных странах, а ее целью является обеспечение информационного первенства в сфере международной безопасности. Выделяют пять моделей системы информационной сохранности:

Модель 1 – установление абсолютной системы защиты от любого типа наступательной информационной, определяющей объективное преимущество

потенциальной информационной войны, заставляя остальные государства изыскивать союзников. В то же время система, строго контролирующая информационное оружие противника, может использоваться на основе потенциальных международных документов, касающихся информационной безопасности.

Модель 2 - предоставление полной информации о существенных преимуществах потенциальных инициаторов информационных войн, использования информационного влияния для уничтожения оборонных систем противника и использования определенного информационного оружия для координации с союзниками для выяснения источника и типа информационных угроз со стороны противника.

Модель 3 - Существование многих стран, раскрывающих информацию, и их потенциальное противостояние определяют сдерживающий фактор для предотвращения расширения информационных угроз и обеспечивают доминирование одной из стран в области международной информационной безопасности, что важно. Глобальное информационное поле и безопасность информации оказали большое влияние на приоритетность решения глобальных проблем.

Модель 4 – Все враждующие субъекты применяют прозрачность информации для создания ситуативного альянса для реализации преимуществ и принятия решений, которые могут препятствовать техническому руководству, и используют способность информационной инфраструктуры в определенных регионах для организации внутренних сил.

Модель 5 – противостояние между международным обществом и международной организованной преступностью, которое может контролировать политический, экономический, социальный и даже прогресс цивилизации [44].

Информационное оружие имеет мощную способность сочетаться с другими традиционными и технологически новыми военными методами, поэтому потенциальное бесконтрольное использование некоторых может быть

губительным для человека. Поэтому только многостороннее сотрудничество между разными государствами может обеспечить решение новых и комплексных вопросов информационной эры во всем мире и установить полную международную безопасность.

Особенностью информационного века являются стремительные изменения в различных сферах жизни, изменения в нескольких экономически-социальных системах, и с течением времени каждая система сталкивается со своими трудностями и ограничениями.

Теория международной информационной безопасности определяет ключевые системы, которые первыми используются в случае информационной борьбы. Наиболее уязвимы политическая, социальная, экономическая, военная, технологическая и духовная сферы общества.

Информационная безопасность в политическом поле включает в себя все элементы национальной и социальной политической системы: система подготовки и принятия решений, система местного и регионального управления, система выборов, специальная информационная и телекоммуникационная государственные системы [50].

В области экономики существует несколько важных систем, включающих общий экономический анализ и предвидение экономического роста, управления и координации действий, а также принятие решений в экономической отрасли, особенно в чрезвычайных ситуациях, в ключевых системах (энергетики, связи, информации).

Опыт развитых государств в информационной сфере показывает, что экономическое преимущество современного мира базируется на постепенном расширении информации, а наиболее быстро развивающиеся страны в направлении информационной цивилизации займут мировую экономическую систему, где международная конкуренция со странами с отсталыми технологиями будет несущественной.

Информация легче всего влияет на общественное достояние, поскольку она включает в себя формирование мнений общественности, информационную

и организационную структуру партий, общественные движения, государство, культурные и религиозные учреждения, основные права и свободы, независимость разнообразия и высказываний и идей.

Угрозы информации в области науки и техники стали глобальными угрозами, от явления трансграничного потока интеллектуальных ресурсов, другими словами, вывод информации с уникальными технологическими свойствами на биологические носители, до разработки международных систем мониторинга, анализируя и прогнозируя научные тенденции доступа к частным и банковским данным [40].

Решающее значение для защиты науки и техники имеют структура наращивания информации, институтов и структур фундаментальных и прикладных исследований, права интеллектуальной собственности, оригинальных идей и запатентованной информации. Информационно-технологические аспекты безопасности сосредоточены на реализации мер, направленных на модернизацию науки и техники и эффективную защиту ресурсов знаний.

В военной области информационными ресурсами вооруженных сил: военно-промышленные комплексы, системы военного управления, контроля и постоянного мониторинга, а также каналы для получения стратегической, оперативной и разведывательной информации.

Важное проявление информационных факторов в международной безопасности кардинально изменило общую оценку доктрин информационной безопасности и положения большинства стран, реализуя таким образом потенциал информационных угроз и необходимость создания соответствующих международных механизмов для контроля информационных конфликтов. Статус развитых стран определяется высокой степенью внимания к информации, правильно рассматриваемой как один из основных факторов собственности в нынешнем мире, а именно:

1. Признание проблемы международной информационной безопасности как гипотетического силового противостояния;

2. Перенос концепции международной информационной безопасности на региональный или тематический уровень;

3. Выделение по комплексной проблеме международной информационной безопасности таких составляющих, как уголовные и международные информационные угрозы и создание международного механизма контроля подобных информационных преступлений;

4. Создание специального Международного суда по информационной преступности; совместные разработки технологии глобальной защиты от информационной угрозы [18].

Поэтому вопросы международной информационной безопасности являются важной частью основных вопросов национальной, региональной и глобальной политики в области международных информационных отношений, а также проявлением новых глобальных вызовов и тенденций в процессе углубления глобализации коммуникаций [49].

Кибербезопасность признается частью информационной безопасности, которая направлена на защиту цифровых активов, а информационная безопасность нацелена на информацию, независимо от того, находится ли она в цифровом или физическом пространстве. Поскольку киберпространство быстро развивается, как информационная безопасность, так и кибербезопасность должны постоянно обновляться, чтобы соответствовать самым последним изменениям [38].

Кибербезопасность описывается как отсутствие конфликта между субъектами таким образом, который способствует безопасности и стабильности в киберпространстве, обеспечивая при этом обмен информацией и экономический обмен. Взгляд на кибербезопасность с этой точки зрения лучше отражает тот факт, что это глобальная проблема безопасности, и в результате все пользователи киберпространства уязвимы для кибератак. Из-за интегрированного существования кибербезопасности правильнее думать о ней как о транснациональной проблеме, в которой правительства сотрудничают для создания стабильного киберпространства [26].

За последние два десятилетия правительства приложили значительные усилия для разработки стратегий кибербезопасности и создания наступательного и оборонительного потенциала в своих регионах. Правительства, с другой стороны, пытались найти баланс между возросшим движением денег, людей, товаров и услуг, с одной стороны, и мерами безопасности, принятыми для защиты основных средств и национального имущества, с другой. Важность поиска сетевой безопасности иллюстрирует некоторые из основных противоречий между международным соперничеством и сотрудничеством в повышении кибербезопасности, даже несмотря на то, что сохранение этого баланса уже давно является частью внешней политики правительства и международных отношений. Тем временем, некоторые международные организации, такие как Организация экономического сотрудничества и развития (ОЭСР), сыграли активную роль в формировании сотрудничества между своими членами для предотвращения вреда сети и создания «общей культуры безопасности» [21].

На самом деле некоторые организации выразили озабоченность своих членов по поводу сетевой безопасности, как в телекоммуникациях, так и в интернет-коммуникациях, и предприняли шаги для их решения. В последние годы в различных кругах обсуждалась желательность и целесообразность сотрудничества правительств и создания совместных институтов для укрепления кибербезопасности.

Таким образом, можно сделать вывод, что, хотя кибербезопасность и информационная безопасность тесно связаны друг с другом и пересекаются в некоторых аспектах, основное различие связано с информацией. Информационная безопасность сосредоточена для защиты информации везде, в то время как кибербезопасность сосредоточена на защите информации в киберпространстве [28].

Сотрудничество между государствами в сфере информационной безопасности необходимо, поскольку оно может ограничить деятельность неправительственных субъектов и киберпреступников. Государства могут быть

не в состоянии согласовать все условия совместного соглашения о кибербезопасности, но они могут согласовать раздел соглашения, касающийся конкретных видов преступного поведения. Договор с общим соглашением о кибербезопасности также может распространять действия правительства в Интернете на закон войны; другими словами, он может определить, как правительства могут использовать киберресурсы и технологии как в отсутствие официальной войны между ними, так и в случае ее. Атаки на сети, а также на подключенные к сети системы управления могут привести к прямому физическому ущербу для людей и объектов, и, как следствие, организации, отслеживающие межгосударственные войны, должны рассматривать эти атаки как иностранные конфликты.

## 1.2 Международно-политическое взаимодействие государств в сфере информационных отношений

Базовым измерением современных конфликтов стало информационное противоборство. Сегодня уже не существует вооруженных международных конфликтов, в которых не используются дополнительные механизмы информационного влияния, пропаганды или информационных технологий. Уязвимость, взаимосвязанность, доступность и незащищенность субъектов международных отношений присущи системному кризису международной информационной безопасности. Неотложным и актуальным является вопрос выработки действенных механизмов обеспечения международной информационной безопасности. Организация Объединенных Наций как институт глобального управления способна обеспечить комплексное решение политической проблемы информационной безопасности при широком представительстве и максимальном учете позиций и интересов всех стран мира.

Международное сотрудничество в сфере информационной безопасности обусловливает необходимость поиска совместных решений в рамках

международных организаций по противодействию информационным и киберугрозам, выработки общей стратегии информационной безопасности для противодействия кибервойнам, информационному терроризму и информационной преступности Международное сообщество пришло к согласию, что только совместными усилиями и на основе международного права возможно решить проблемы в политической, экономической, безопасности и других сферах жизнедеятельности общества [17].

Организация Объединенных Наций как институт глобального управления способна обеспечить комплексное решение политической проблемы информационной безопасности при широком представительстве и максимальном учете позиций и интересов всех стран мира. Деятельность ООН в сфере информационной безопасности направлена на разработку международно-правовой базы и выработку документов для противодействия противоправному использованию научно-технического и технологического прогресса террористическими группировками и организованной преступностью. Проблема информационной безопасности в контексте формирования глобального информационного общества стала актуальной для деятельности специализированных учреждений ООН, в частности, ЮНЕСКО и МСЭ, учитывая гуманитарные и технические программы и проекты организаций [20].

Одной из первых встреч на международном уровне по развитию информационного общества и обеспечения безопасности стала конференция «Информационное сообщество и развитие», состоявшейся в Мидранде (ЮАР) 13-15 мая 1996 года [34].

30 июля 1996 года в Париже состоялось совещание на уровне министров иностранных дел и министров по проблемам терроризма. Был проведен глубокий анализ новых тенденций, связанных с терроризмом во всем мире. По результатам работы международной конференции был принят заключительный документ, где содержался призыв к странам принимать меры, которые при уважении основных свобод и верховенства права были бы направлены на

эффективную борьбу с терроризмом. В документе содержался призыв рассмотреть вопрос об опасностях, связанных с использованием террористами сетей и систем передачи информации с целью преступной деятельности, и необходимости нахождения средств для предотвращения таких действий. Отдельный раздел заключительного документа был посвященный укреплению международного сотрудничества в деле борьбы с терроризмом путем присоединения к международным конвенциям и протоколам, касающихся борьбы с терроризмом, путем оказания помощи и поддержки правительств других стран, путем подписания двух- и многосторонних соглашений, развития сотрудничества между правоохранительными органами с целью предотвращения и выявления террористических актов [31].

В сентябре 1998 года Российская Федерация и Соединенные Штаты Америки подписали Совместное заявление президентов «Об общих вызовах безопасности на рубеже XXI века». Проект документа предусматривал совместное определение вызовов и угроз в этой сфере, выработку понятийного аппарата, вынесение вопроса о глобальной информационной безопасности на рассмотрение ООН, а также разработку международного многостороннего договора о борьбе с информационным терроризмом и преступностью. Обсуждение проекта заявления не привело к сближению сторон, но в общем виде информационная безопасность была упомянута в Совместном заявлении «Об общих вызовах безопасности на рубеже XXI в.» Заявление было распространено в качестве документа ГА ООН и предварительной повестки дня и документа Совета Безопасности [30].

Конференции в Мидранде, Париже и Совместное заявление президентов стали исторической основой и предвестниками принятия в 1998 году на 53 сессии Генеральной Ассамблеи ООН Резолюции A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [2]. Именно в резолюции 53/70 впервые на самом высоком уровне отмечается, что новые технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной

стабильности и безопасности, и могут негативно влиять на безопасность государств. В резолюции содержится призыв к государствам-членам ООН способствовать рассмотрению на международном уровне существующих и потенциальных соглашений в сфере информационной безопасности, разработать международные принципы, направленные на укрепление глобальных информационных и телекоммуникационных систем и на борьбу с информационным терроризмом и криминалом. В Резолюции содержится призыв ставить на повестку дня будущих сессий пункт «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и просьба ко всем государств-членов информировать о своей точке зрения относительно общей оценки проблем информационной безопасности. О таких оценках страны-члены должны информировать Генерального секретаря ООН, которому поручено представить соответствующий доклад на следующей сессии Генассамблеи ООН.

Доклад Генерального секретаря был опубликован в 1999 году (А /54/213) [8]. Он состоял из оценок Австралии, Белоруссии, Брунея, Великобритании, Катара, Кубы, Омана, России, Саудовской Аравии и США. Объединяющим фактором для этих оценок было признание наличия проблемы, но проявились существенные различия в расстановке акцентов (военная, правовая, гуманитарная или другие составляющие), в методике ее рассмотрения и путях решения.

Резолюция 53/70 положила начало широкому обсуждению вопросов международной информационной безопасности и поиска стратегий обеспечения безопасности субъектов международных отношений от новых угроз. Генеральный секретарь ежегодно предоставляет Генеральной Ассамблее доклад, содержащий позиции государств - членов Организации Объединенных Наций по данной теме.

Еще одним важным этапом для рассмотрения вопроса международной информационной безопасности стала Всемирная встреча на высшем уровне по вопросам информационного общества (первый этап - 2003 г., Женева, второй

этап - 2005 г., Тунис) и Всемирная встреча на высшем уровне по вопросам информационного общества ВСИО+10 2015 г., которая проходила под эгидой ООН. Конференция предложила мировому сообществу рассмотреть существующие и потенциальные угрозы для безопасности информационных и коммуникационных сетей, объединить усилия государств-членов ООН, направленных на оценку состояния информационной безопасности, а также на перспективную разработку международной конвенции по информационной безопасности.

Основой для такого решения стали соответствующие положения итоговых документов региональных конференций по подготовке Всемирной встречи, а именно общеевропейской, азиатско-тихоокеанской, африканской, западно-азиатской и латиноамериканской, в которых была заложена основа для дальнейшего обсуждения проблематики международной информационной безопасности на уровне ООН.

Проблематика международной информационной безопасности вошла в итоговые документы женевской встречи ВСИС – Декларации принципов «Построение информационного общества – глобальная задача нового тысячелетия». В частности, в Декларации принципов (раздел «Укрепление доверия и безопасности при использовании ИКТ») отмечается, что международная информационная безопасность и безопасность информационной инфраструктуры являются необходимой предпосылкой становления глобального информационного общества и преодоления асимметрии информационного развития. Необходимо отметить, что повышение доверия и безопасности при использовании информационно-коммуникационных технологий, учитывая их двойную природу, определяется в документе как стратегия глобальной культуры кибербезопасности, которая должна обеспечиваться посредством международного сотрудничества всеми заинтересованными сторонами и компетентными международными организациями. Такие усилия, по мнению международных экспертов по проблемам информационной безопасности, должны опираться на широкое

представительство в разработке международно-правового документа информационно развитых и информационно бедных стран для обеспечения равенства, суверенности и доступа к глобальным информационным ресурсам, что обусловливает защиту частной жизни и прав человека, трансграничного сотрудничества в сфере экономики, торговли, культурных обменов и социальных гарантий. Политическим итогом обсуждения проблемы международной информационной безопасности на форуме ВСИС стало признание принципов всеобщего и недискриминационного доступа к высоким технологиям для всех наций, поддержка деятельности ООН, направленной на обеспечение международного мира и стабильности, предотвращение применению информационных вооружений, способных негативно повлиять на территориальную целостность, инфраструктуру и массовое сознание любого государства [45].

Проблема информационной безопасности в Плане действий рассматривается в контексте конкретных мероприятий по укреплению доверия и безопасности при использовании ИКТ, среди которых главное внимание уделено: углублению международного сотрудничества в рамках ООН и в рамках других международных форумов с целью анализа существующих и потенциальных информационных угроз, а также решения политических, правовых, экономических, социальных, культурных, военных, технологических и экологических вопросов информационной безопасности; разработке законодательства, что делает возможным эффективное расследование неправомерного использования ИКТ; содействию международному взаимодействия в информационной сфере, а также превентивному предупреждению негативных информационных воздействий; поощрению активного участия заинтересованных стран в разработке политических, программных и правовых документов на уровне ООН. Особый акцент сделан на важности международного сотрудничества между государствами в рамках ООН, поскольку именно государственные органы в сотрудничестве с частным

сектором должны предупреждать, выявлять и реагировать на проявления киберпреступности и злоупотребления высокими технологиями.

Дальнейшее развитие международного сотрудничества в сфере информационной безопасности нашло свое воплощение в политических дискуссиях и документах тунисской встречи по информационному обществу, во время которой оказались острые противоречия между подходами ООН и большинства государств-членов организации и США, поскольку именно позиция наиболее мощного информационной державы касалась лишь признания проблемы глобальной культуры кибербезопасности и противодействия рассмотрению высоких технологий как технологий двойного назначения и оружия массового поражения. В Тунисском обязательстве 2005 г. была подтверждена позиция ООН относительно потенциала ИКТ как фактора предотвращения конфликтов, а также содействие их мирному урегулированию, по поддержке гуманитарных акций, включая защиту гражданских лиц в вооруженных конфликтах, деятельность миссий по поддержанию мира и оказание помощи в миростроительстве в постконфликтный период [41].

Зато в Тунисской программе для информационного общества было поддержана инициатива США и других развитых государств по внедрению стратегии глобальной культуры кибербезопасности, которая требует национальных действий и активизации международного сотрудничества на региональном уровне. Политико-правовые аспекты глобальной культуры кибербезопасности усматриваются в противодействии киберпреступности, совершенные в рамках юрисдикции одной страны, но имеющих последствия в других, в необходимости действенных и квалифицированных инструментов и действий на национальном и международном уровнях.

В Тунисской программе для информационного общества указывается на углубление сотрудничества в сфере информационной безопасности в рамках АТЭС, ОЭСР и МСЭ, что демонстрирует комплексный подход к противодействию новейшим информационным угрозам на уровне законодательства, деятельности правоохранительных органов, разработки

технических мероприятий и тому подобное. В документе подтверждается приверженность к обеспечению фундаментальных прав и свобод в информационной сфере, в частности, относительно поиска, получения, распространения и использования информации и знаний. Государства-члены ООН и участники всемирного форума в Тунисе подчеркнули важность борьбы с терроризмом во всех его формах и проявлениях в Интернете наряду с соблюдением прав человека и призвали правительства всех стран и мировое сообщество подтвердить право каждого человека на доступ к информации в соответствии с Женевской Декларацией принципами и другими международными документами.

На 71-й сессии ГА ООН 19 июля 2016 года был принят доклад Генерального секретаря «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». В докладе представлены официальные отчеты правительств 19 государств для укрепления международной безопасности и содействия международному сотрудничеству в этой сфере [24].

На 72-й сессии ГА ООН 11 августа 2017 года был принят доклад Генерального секретаря «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», как выполнение рекомендаций резолюции A/RES/71/28 от 5 декабря 2016 года относительно информирования стран о своей точке зрения по вопросам общей оценки международной информационной безопасности и усилий, которые прилагают государства. Резолюцию поддержали 181 страна. Против никто не голосовал [30].

В докладе представлены официальные отчеты правительств 23 государств для укрепления международной безопасности и содействия международному сотрудничеству в этой сфере.

Многие страны и территории укрепили свои стратегические планы по защите от интернет-угроз. С 2016 года многие страны опубликовали или обновили свои стратегии по защите от интернет-угроз. Они опубликовали

правила и законы, учредили специальные агентства, усовершенствовали рабочие механизмы, запустили просветительские и образовательные инициативы в области интернет-безопасности, способствовали распространению культуры безопасности в Интернете и нарастили свой потенциал и укрепили международное сотрудничество.

В конце XX века вопросы кибербезопасности вышли на уровень дипломатических ведомств и высших руководителей государств. В 2015 были подписаны соответствующие документы между РФ и КНР, КНР и США, КНР и Великобританией, в рамках которых страны обязуются не только сотрудничать, но и не допускать атаки друг на друга. Активно обсуждаются недавние поправки к Вассенаарским соглашениям по ограничению экспорта шпионского программного обеспечения. Одной из главных новелл последних лет стало также использование незащищенных почтовых сервисов политиками всего мира Международное сообщество инициативно реагировало на киберпреступления и кибертерроризм. Киберпреступления и кибертерроризм были признаны серьезной проблемой для всеобщего мира и безопасности. Многие государства теперь с помощью механизмов международного сотрудничества в области права и безопасности взяли на себя обязательства эффективно бороться с киберпреступлениями и кибертерроризмом, тщательно следя за тем, чтобы технологии, коммуникации и ресурсы не использовались для преступлений и террора, и искоренять возможности для распространения террористической и экстремистской идеологии в интернете. Было достигнут значительный прогресс в разработке норм двустороннего и многостороннего сотрудничества в деле борьбы с преступлениями в сфере Интернета.

Большинство стран уделяет большое внимание вопросам информационной безопасности, регулированию сети интернет, формированию общепринятых международных правил и норм признавая потребность в сотрудничестве и взаимном согласии, основанных на Уставе ООН, международном законодательстве и базовых принципах международных отношений. Стремление достичь устойчивого, стабильного и безопасного

общества объединило международное сообщество, подтолкнуло к партнерству, сотрудничеству и взаимопониманию. Многостороннее участие стало признаком процесса обеспечения международной информационной безопасности. ООН активно включилась в процесс содействия глобальному развитию и построению безопасного мирового общества.

Таким образом, можно заключить, что тема международного сотрудничества в вопросах обеспечения международной безопасности вообще и информационной безопасности в частности, стала острой и актуальной в современном мире. Международное сообщество в рамках международных организаций и благодаря механизмам ООН демонстрирует стремление к масштабному сотрудничеству, объединению усилий, взаимодействию, совместному участию, открытости и прозрачности, ответственности и инновационности в решении общей проблемы безопасного мира.

# 2 Анализ влияния деятельности международных организаций на обеспечение международной информационной безопасности

## 2.1 Политика ООН в области обеспечения международной информационной безопасности

В рамках современности, дополненной увеличением рисков и конфликтов в пространстве общественного и политического взаимодействия, особо остро стоит проблема обеспечения международной информационной безопасности. Это связано также с тем фактом, что глобальные акторы, будь то государства, ТНК, неправительственные объединения способны использовать аспекты ИКТ в своих политических и иных видах целях. Неконтролируемое использование коммуникационных технологий чреваты проблемами манипулирования и подтасовкой информации в глобальном масштабе.

Что касается методов противодействия по отношению кибератак, то исследователи, к примеру, отмечают метод «сдерживания геополитических соперников» [36, с. 56], его воплощением оказывается способность государств в осуществлении ответных мер военного толка. Тем не менее, представляется также очевидной проблема того, что подобный сценарий развития событий чреват повышения напряжения международного взаимодействия. Этот аспект нашел своей отражение и в работе ГПЭ ООН по достижениям в области информатизации и коммуникации, которая подчеркнула, что феномен быстрого развития ИКТ охватывает один из сегментов международных отношений [62].

Специфика информационной области взаимодействия общества в рамках различных способов коммуникации заключается в том, что она отличается от других форм взаимодействия людей, регулируемых международным и национальным законодательством. Следствием появления глобальных форм коммуникации становится тот факт, что тиражируемая и создаваемая информация нарушает территориально-временную обусловленность.

В связи с чем, одной из форм геополитической силы оказывается достижение геополитических конкурентных преимуществ, заключающихся в наличии первенства в развитии передовых информационных технологий.

Для предотвращения подобного рода проблем под эгидой ООН была создана первая группа правительственных экспертов (далее ГПЭ) в 2001 году в соответствии с решением 56-й сессии Генеральной Ассамблеи ООН по инициативе России. Работа первой ГПЭ началась в 2004 году. Принятие решений в рамках ГПЭ основывалось на принципе консенсуса.

Однако доклад первой ГПЭ не был одобрен из-за особой позиции Соединенных Штатов, которые были единственной страной среди 15 государств-членов, не поддержавшей его. Соединенные Штаты выступили против включения в документ положения о военно-политическом измерении угроз международной информационной безопасности, не желая ограничивать себя в военном развитии ИКТ.

В начале 2000-х годов Соединенные Штаты не видели необходимости брать на себя международные обязательства, которые могли бы ограничить их потенциал в этой области. Соединенные Штаты поддерживали международное сотрудничество в противодействии криминальным и террористическим угрозам в рамках международных институтов с ограниченным составом государств-«единомышленников», таких как «Группа восьми» (G-8). В 2000 году G-8 приняли Окинавскую хартию Глобального информационного общества, которая признавала только существование террористических и криминальных угроз кибербезопасности.

ГПЭ возобновила свою работу в 2009 году. Во время трехлетней паузы в ее работе с 2006 по 2008 год Россия выдвинула проекты резолюций «Достижения в области информации и Телекоммуникации в контексте международной безопасности» на 61-й, 63-й и 63-й сессиях Генеральной Ассамблеи ООН.

Эти документы отражали российское видение угроз в области ИКТ и были приняты, несмотря на сопротивление со стороны Соединенных Штатов.

Стоит отметить, что за этот период появились соавторы проектов резолюций, выдвинутых Россией (10, 17 и 28 соответственно) – и не только из числа традиционных союзников Российской Федерации по Содружеству Независимых Государств (СНГ), (ОДКБ), ШОС и БРИКС, но и от ряда других государств.

Одним из краеугольных камней доклада стал вопрос о его терминологической специфике. Этот аспект связан с тем, что государства в публичном поле используют различные понятия, к примеру, термин «информационная безопасность» или же «кибербезопасность». Несмотря на данную проблему, эксперты смогли наладить диалог, придя к общему знаменателю касательно ключевых пунктов доклада. Тем самым в его тексте можно встретить такие понятия как: «информационная безопасность» и «безопасность при использовании ИКТ»».

Результатом работы ГПЭ под председательством России стало утверждение доклада, который был согласован 16 июля 2010 года всеми 15 государствами - членами группы [11]. В докладе ГПЭ были определены существующие и потенциальные угрозы безопасности ИКТ и квалифицированы как одна из наиболее актуальных проблем XXI века.

Среди угроз, выявленных в докладе, были: растущая уязвимость критически важной информационной инфраструктуры в результате незаконного использования ИКТ, сложность в предупреждении кибератак, риске использования ИКТ в качестве инструмента войны и тайной разведки, а также их использовании в политических целях, в том числе через посредников, представленных отдельными лицами, группами или организациями.

Одним из ключевых тезисов доклада оказалось обобщение существенных рекомендаций по предотвращению угроз, которые сопутствуют использованию ИКТ. Работа второй ГПЭ была оценена с точки зрения резолюции «Достижения в области информатизации и телекоммуникаций в контексте международной безопасности», разработанной Российской Федерации и принятый в декабре 2010 года Генеральной Ассамблеей ООН [9]. Было принято решение созвать новую группу в 2012 году.

Перед созывом новой ГПЭ Россия провела эффективную подготовительную работу в кругу своих союзников по Шанхайской организации сотрудничества (ШОС). В частности, к 2011 году партнеры по ШОС разработали совместный документ, направленный на консолидацию принципов государственной деятельности в сфере ИКТ. На 66-й сессии Генеральной Ассамблеи ООН Российская Федерация и страны ШОС представили официальный документ «Правила поведения в области международной информационной безопасности» [13], который сыграл важную роль в запуске работы новой ГПЭ, которая начала свою работу в 2013 году.

Международный политический контекст подчеркнул важность угроз международной информационной безопасности. Например, в 2010 году вирус «Stuxnet» атаковал ядерную инфраструктуру Ирана. А в 2011 году в Северной Африке и на Ближнем Востоке прошли массовые протесты, которые в СМИ назвали «революциями Facebook».

Эти события подчеркнули важность угроз ИКТ для глобальной безопасности и необходимость гармонизации правил и безопасного использования ИКТ. В 2013 году 15 государств - членов ГПЭ единогласно приняли итоговый доклад, в котором были отражены меры по повышению прозрачности, безопасности, стабильности и укреплению доверия и потенциала (в первую очередь в развивающихся странах) [11].

Кроме того, было подчеркнуто, что при сохранении координирующей роли государства необходимо активизировать участие частного сектора и гражданского общества в обсуждении вопросов международного сотрудничества в этой области. В докладе ГПЭ отмечается, что Устав ООН и существующие нормы международного права должны использоваться для регулирования деятельности государств в среде ИКТ.

В то же время особенности технологий (их глобальный характер, возможность сохранения анонимности при их использовании, всеобщая доступность, невозможность четкой идентификации субъекта, ответственного за кибератаку, и т.д.) означают, что действующая международно-правовая база

остается недостаточной. В связи с этим документ предусматривал возможность разработки в будущем дополнительных норм для регулирования отношений в информационной сфере. Еще одним направлением будущего взаимодействия, закрепленным в докладе за 2013 год, является задача создания и поддержания регулярного институционального диалога по вопросам международной информационной безопасности под эгидой Организации Объединенных Наций и в рамках других форумов.

Однако конкретные параметры возможного диалога указаны не были. стороны провели традиционную оценку существующих и потенциальных угроз информационной безопасности, включили положения о нормах, правилах и принципах ответственного поведения государств, а успех третьей ГПЭ способствовал принятию решения продолжить обсуждения с целью достижения более существенных соглашений в рамках новой группы экспертов.

Следующий этап сотрудничества в рамках ГПЭ относится к декабрю 2013 года, когда 68-я сессия Генеральной Ассамблеи ООН приняла российский проект резолюции «Достижения в области информатизации и телекоммуникаций в контексте международной безопасности» [12].

В документе приветствовалась эффективная работа предыдущей ГПЭ и содержалась просьба о том, чтобы четвертая ГПЭ начала свою работу в 2014 году в расширенном составе с участием представителей 20 стран. В отличие от предыдущей группы, задачи новой ГПЭ были более конкретными: ключевым пунктом повестки дня было не изучение всего спектра угроз в области международной информационной безопасности, а скорее изучение проблем использования ИКТ в конфликтах и применимости международного права к информационной сфере.

Несмотря на острые разногласия, сопровождавшие обсуждение в рамках четвертой ГПЭ, участники группы представили итоговый отчет 26 июня 2015 года. Несмотря на узкий круг задач ГПЭ, анализ текущей ситуации в области международной информационной безопасности был многогранным и отразил основы российского подхода к этому вопросу.

Доклад помимо прочего включал в себя информацию, декларирующую идею развития форм и средств борьбы с кибератаками и необходимость регулирования конфликтов в информационном пространстве. Для государств, например, в этой связи ориентиром для урегулирования конфликтов оказались общепризнанные принципы международного права при использовании ИКТ.

В этом отношении государства были гарантами безопасности своего информационного пространства и несли ответственность за предотвращение его использования другими субъектами с целью совершения противоправных действий. В документе отражен важный элемент российского подхода к проблемам международной информационной безопасности, а именно необходимость обоснования любого рода обвинений, которые выдвигаются против государства в совершении незаконных действий в сфере ИКТ.

Что касается общих вопросов применимости международного права к информационному пространству, эксперты ГПЭ подтвердили возможность разработки новых правовых норм с учетом специфики технологий.

Кроме того, в итоговом докладе были намечены перспективные области для дальнейшей работы, которые включали коллективную и индивидуальную разработку государствами концепций обеспечения международного мира и безопасности при использовании ИКТ на правовом, техническом и политическом уровнях, а также расширение сотрудничества на региональном и многостороннем уровнях для содействия общему согласию в вопросах в области ИКТ.

В связи с успехом четвертой ГПЭ на 70-й юбилейной сессии Генеральной Ассамблеи ООН 23 декабря 2015 года консенсусом была принята резолюция «Достижения в области информатизации и телекоммуникаций в контексте международной безопасности», разработанная Россией в соавторстве с 84 государствами. В документе обозначена возможность продолжения работы ГПЭ в 2016-2017 годах.

Накануне запланированного начала работы новой группы в 2015 году обновленная версия текста правил, ранее разработанных в рамках ШОС, была

распространена от имени государств - членов организации в качестве официального документа Генеральной Ассамблеи ООН по инициативе Российской Федерации [58]. Под влиянием международной политической ситуации («разоблачения» Эдварда Сноудена о практике сбора и анализа личной информации граждан различных стран со стороны правительства США), в правила был добавлен расширенный раздел, посвященный правам человека.

Однако, несмотря на позитивные сигналы, предшествовавшие работе новой группы под председательством немецкого эксперта К. Гейер, шестая ГПЭ не смогла подготовить итоговый доклад из-за фундаментальных разногласий между участниками (Соединенными Штатами и их союзниками, с одной стороны, Россией и странами-единомышленниками - с другой) относительно подходов и принципов будущего регулирования глобального информационного пространства.

Кроме того, негативная динамика в отношениях между Россией и Соединенными Штатами, наряду с бездоказательными обвинениями со стороны Соединенных Штатов в адрес России во вмешательстве во внутренние американские выборы, касается также всех стран, независимо от их уровня технологического развития.

Запад (прежде всего Великобритания, Канада и Нидерланды) во главе с Соединенными Штатами стремился закрепить «право сильного», а концепция силовых контрмер (в том числе в обход ООН) препятствовала конструктивному диалогу. Россия при поддержке 11 государств (Бразилии, Китая, Кубы, Египта, Индии, Индонезии, Казахстана, Кении, Сенегала и Сербии) настаивала на недопустимости развязывания гонки вооружений в информационном пространстве и превращения его в арену новых войн. В нем также указывалась важность формирования справедливого и равноправного миропорядка, отражающего интересы Совета Безопасности в информационном пространстве.

Они также попытались отнести киберпространство к сфере военных действий и сделать возможным применение определенных международно-правовых норм, в том числе норм международного гуманитарного права, к актам насилия в информационном пространстве. В то же время они пренебрегли проблемой идентификации источника в вопросах кибератак.

ГПЭ завершила свою работу в мае 2021 года принятием своего окончательного доклада. В соответствии с мандатом группы, в документе основное внимание уделяется применимости международного права к информационной сфере. В нем содержатся подробные разъяснения по ранее достигнутым соглашениям (изложенным в итоговых отчетах за 2010, 2013 и 2015 годы).

В новом докладе раскрывается содержание норм, регулирующих деятельность государств в киберпространстве, и рассматриваются меры, необходимые для их эффективного осуществления. В докладе подчеркивается, что нормы и принципы международного права, в частности Устава ООН, применимы к среде ИКТ, в то время как международное гуманитарное право применимо только в условиях вооруженного конфликта. Однако в докладе не был указан порог вооруженной агрессии. В то же время отмечается, что необходимо продолжить дискуссию о применимости международного права к информационной сфере.

Подводя итог, следует отметить, что предложенный Россией формат открытого диалога по безопасности ИКТ продемонстрировал свою эффективность и актуальность в решении насущных проблем, стоящих перед международным сообществом. Работа ГПЭ помогла повысить доверие и взаимопонимание между государствами, но раскол в позициях не был преодолен полностью, о чем свидетельствуют альтернативные проекты в области сотрудничества по безопасности ИКТ, предложенные западными странами.

## 2.2 БРИКС, ШОС и ОДКБ как гарант международной безопасности в информационном пространстве

Что касается положений ШОС касательно международной информационной безопасности, то организация перенесла свои дипломатические идеи уважения суверенитета, невмешательства во внутренние дела государств, равенства и взаимоуважения в выполнении международных норм (без двойных стандартов) и борьбы с сепаратизмом, экстремизмом и терроризмом в киберпространстве.

На самом деле, интересно, что в соответствии с китайским и российским видениями безопасности ШОС предлагает информационную безопасность воплощенную в Соглашении между правительствами государств-членов Соглашение ШОС о сотрудничестве в области обеспечения международной информационной безопасности, подписанное Китаем, Россией, Казахстаном, Кыргызстаном, Таджикистаном и Узбекистаном как эквивалент того, что Западные страны называют кибербезопасностью.

Соглашение в области информационной безопасности было заключено в 2009 году после последствий кибератак в Эстонии (2007) и во время конфликта в Грузии (2008). И во второй статье в нем отражены следующие угрозы:

1. разработка и применение информационного оружия и подготовка к ведению информационной войны;
2. информационный терроризм;
3. информационное преступление;
4. использование доминирующего положения в киберпространстве в ущерб интересам и безопасности других государств;
5. распространение информации, наносящей ущерб политическим системам;
6. природные и/или антропогенные угрозы безопасному и стабильному функционированию глобальной и национальной информационной инфраструктуры [14].

Таким образом, в дополнение к идеям ШОС, заложенным в этих представлениях, критикуется модель управления киберпространством, сосредоточенная в Соединенных Штатах. Определения войны и информационного терроризма — в приложениях к документу — становятся очень близкими к китайско-российским представлениям, в то же время испытывая влияние многостороннего подхода и взаимного доверия [14]. Кроме того, существует предложение о международном участии в дебатах по кибербезопасности/информационной инфраструктуре. Это международное взаимодействие уже можно увидеть в двух моментах в рамках Организации Объединенных Наций.

Первое состоялось 12 сентября 2011 года, когда четыре члена ШОС (то есть Китай, Россия, Таджикистан и Узбекистан) представили Организации Объединенных Наций проект Международного кодекса поведения в области информационной безопасности Генеральной Ассамблеи, который был отклонен. Второй момент был в 2015 году, когда шесть членов ШОС представили Генеральной Ассамблее ООН новый проект кодекса, который также был отклонен.

Этот отказ был основан на восприятии идей чрезмерного государственного контроля над киберпространством. Тем не менее, это важно подчеркнуть, что документ также предлагал подход равных прав в рамках новых рамок международных соглашений, в области киберпространства.

Следовательно, представляя противоположный взгляд в отношении международного права вопреки взглядам стран НАТО, поскольку те выступают за использование существующей развитой системы международного права с незначительными изменениями, предложенными в Таллиннском руководстве, подготовленным Центром передового опыта НАТО в области кибернетического сотрудничества и обороны (CCDCOE).

Информационная безопасность актуальна для членов ШОС, поскольку она имеет практические последствия в экономике стран, особенно в энергетической и транспортной инфраструктурах, которые объединяют

государства. Аналогичным образом, в свете настоящего документа можно сказать, что, несмотря на столкновение между двумя державами в Азиатском регионе, охватываемом ШОС, существует единство взглядов и схожие международные цели. Другими словами, есть модель, по крайней мере, в руководстве Организации, у которой есть структурированный подход по вопросам обеспечения кибербезопасности.

Более того, стоит подчеркнуть, что существует разница между концепцией кибербезопасности и информационной безопасности. Кроме того, взгляды стран-членов ШОС идут вразрез с преобладанием североамериканской проекции осуществления контроля над киберпространством.

Что касается специфики взаимодействия в рамках БРИКС в сфере информационной безопасности, то стоит отметить, что большинство мер необходимых для осуществления и поддержки безопасности в информационном пространстве на национальных уровнях уже существуют. Такие шаги осуществляются членами БРИКС с середины 2010 года. Тем не менее, важнейшие проблемы национальной безопасности в информационной сфере остаются нерешенными для всех стран организации.

Для преодоления этой проблемы, БРИКС необходимо действовать с направлением в формировании единой системы защиты и единого пространства коллективной информационной безопасности БРИКС. При этом ключевым положением, которое может лечь в основу разработки такого пространства и системы обеспечения информационной безопасности в перспективе взаимодействия БРИКС на всестороннем уровне оказывается общая необходимость в предупреждении осуществления транснациональной киберпреступности.

Для эффективного функционирования наднациональной системы обеспечения коллективной безопасности стран БРИКС в информационной сфере необходимо создать наднациональные структуры, которые будут способны осуществлять и обеспечивать вопросы коллективной безопасности БРИКС [42].

Организационная структура подобной системы может выглядеть следующим образом [42]:

1. Главенствующую роль необходимо принять определенному совету стран-участников БРИКС по коллективной безопасности. Представителями такого органа могут быть профессиональные лица, чья деятельность связана с осуществлением информационной безопасности.

2. Также видится целесообразным создание центра кибербезопасности БРИКС, его главной задачей станет создание и поддержка киберпространства стран-участниц объединения. Функционал данной структуры будет включать вопросы предупреждения кибератак и их профилактики.

3. Отдельная структура, занимающаяся вопросами имиджа системы. Его руководство призвано являться своего рода PR-агентом всей системы, среди основных функций которого оказываются налаживание связей и международного сотрудничества.

4. Отдел, связанный с медиа-контентом. Роль которого сводится к обеспечению распространения ключевой информации среди стран-участниц БРИКС, а также уделение внимания по отношению к зарубежной аудитории в интересах реализации комплексных мер и программ информационной безопасности БРИКС.

5. Экспертно-научный отдел, цель которого сводится к изучению и реализации инициатив стран-участниц объединения в контексте обеспечения международной информационной безопасности.

В то же время, нельзя игнорировать и тот факт, что в рамках международных связей и взаимодействия происходит своего рода отход от монопольной модели мирового рынка, с ключевой ролью в его осуществлении Соединенных Штатов. В связи с чем, это открывает простор для интеграционных взаимодействий организаций, в том числе и рассмотренной нами БРИКС. Такие объединения могут занять лидирующие позиции в формируемой полицивилизационной модели международных отношений.

Отдельного упоминания заслуживает и организация ОДКБ. Страны которой сталкиваются с рядом основных общих проблем, с которыми сталкивается государство при разработке своей стратегии информационной безопасности:

1. Границы так называемого «информационного суверенитета» не определены. Государственный суверенитет, как известно, четко определен законодательством, границами государства, международными договорами, то есть институциональными правилами поведения для стран, но в информационном пространстве такие методы разграничения не работают из-за специфики информации и ИКТ как ресурса. На данный момент в конвенциях сформулированы лишь некоторые принципы и подходы, но зачастую не все они поддерживаются или нарушаются.

2. Проблема концептуализации информационной безопасности и информационной войны. Это включает в себя вопрос терминологии, институционализации, что создает значительные трудности в применении мер на практике.

3. Сложность проведения различия между гражданскими и военными целями в области ИКТ. Сама технология не является оружием, а критически важная инфраструктура не имеет статуса военного объекта. Таким образом, на практике вредное использование ИКТ для такой инфраструктуры трудно рассматривать как военные действия.

4. Проблема атрибуции, то есть сложность определения состава, источника угрозы.

Советник Отдела противодействия вызовам и угрозам Секретариата ОДКБ Владислав Шушин также выделил ряд проблем, с которыми организация сталкивается на пути к достижению цели создания единого информационного пространства. По его словам, ни одно государство не может обеспечить свой информационный суверенитет в абсолютной форме. В настоящее время не существует единых, согласованных на международном уровне и поддерживаемых правил поведения в информационном пространстве, а

технические достижения в области защиты информации пока не позволяют полностью защитить ваши информационные ресурсы от несанкционированного доступа [57].

Именно поэтому региональное сотрудничество играет такую важную роль. Формирование общей системы коллективной безопасности напрямую зависит от наличия доверия между государствами. Укрепление доверия является одной из основных тем повестки дня каждого заседания органов ОДКБ, на нем обсуждаются обмен данными, совместные операции, технологическая и кадровая интеграция.

В свою очередь, активный компонент означает, что существует несколько (значимых) организаций, действующих в качестве субъектов информационного пространства, в функции которых входит установление отношений между правительствами и обществом, формирование имиджа региональной группировки и защита ее интересов на мировой арене. Субъектами информационного пространства, с научной точки зрения, являются информационные ресурсы, средства информационного взаимодействия и информационная инфраструктура. Как традиционные, так и онлайн-СМИ представлены на мировом медиа-рынке. В связи с этим усиливается запрос общества на использование информационных ресурсов.

Современные технологии, внедряемые в глобальном Интернете, позволяют освещать события в режиме реального времени практически для всего населения Земли. ОДКБ нуждается в подобной информационной кампании, которая представляла бы регион на мировой арене.

Информационная безопасность является такой же сферой интересов национальной обороны, как и прямые вооруженные угрозы. Особенность этого вида безопасности заключается в том, что сделать его доступным для отдельного государства крайне проблематично, а значит, необходимо срочно обратить на него внимание на региональном уровне. ОДКБ, как организация коллективной безопасности, является наиболее подходящей платформой для мониторинга в области информационной безопасности. Создание единого

информационного пространства позволит нашему региону стать альтернативным, независимым и самостоятельным субъектом в рамках глобальной информационной системы, что на данный момент имеет большое значение. Основой этого информационного пространства должен стать набор сформулированных и оригинальных ценностей, отражающих особенности региона и его исторический путь, а также набор действующих лиц (СМИ), имеющих вес на мировой арене, которые вместе с остальным международным сообществом будут выстраивать свою политическую линию и укреплять региональные позиции в информационной повестке дня [19].

Таким образом, государства представленных организаций нуждаются в разработке концептуальных программ информационной безопасности, определенного соглашения на региональном уровне. Тем не менее, страны стараются проецировать собственное видение в решении вопросов информационной безопасности на интеграционные объединения более высокого порядка, такие как Организация Объединенных Наций, для предложения новых моделей международного законодательства в цифровой сфере.

## 2.3 Проблемы и пути решения в международной информационной безопасности. Сравнение универсального и регионального подходов

Современное состояние межгосударственной системы именуют политической нестабильностью. Характерными чертами такого состояния считают отсутствие со времен Холодной войны какого-либо всеобъемлющего международного договора, закрепляющего новый мировой правопорядок. За этот период не было создано ни одного нового международного института для его поддержания. Существующие международные институты, такие как ООН, НАТО, ВТО в новых условиях постепенно теряют свою эффективность [39]. Постепенно формируются определенные тенденции развития современных

международных отношений, напрямую влияющих на состояние международной безопасности.

Во-первых, усиливается фактор дестабилизации в последние 15-20 лет из-за перераспределения сил в мире. Во-вторых, Азия испытывает небывалый подъем, последствием которого является размораживание старых или появление новых конфликтов: Японии - с соседями, Китая - с Индией, суннитских монархий - с Ираном и т.д. В-третьих, складывается тревожная ситуация в системе международной безопасности, связанная с формированием обратных центробежных направлений развития в военно-технической сфере, обусловленная выходом США г. из Договора по противоракетной обороне (2003 г.), а затем - из ДРСМД (2019 г.). Впоследствии баллистическая ракета средней дальности и наземного базирования, испытанная 12 декабря 2019 года в США, пролетела более 500 км. В результате начинает рушиться основа прежнего режима нераспространения такого оружия.

Еще одним проявлением кризиса международных отношений становится продолжающаяся утрата своего влияния и значимости многими глобальными и региональными международными институтами как в сфере экономики, так и безопасности. Все названные выше проблемы и противоречия вызывают обострение отношений и противостояние в идеологической сфере, усиление ценностных разногласий, информационные войны.

Государства разным образом определяют границы границы информационной безопасности: в России информационная безопасность подразумевает «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [48].

В свою очередь, в США преимущественно применяется термин «кибербезопасность», под которым подразумевается «обеспечение

безопасности информации (как в электронном, так и материальном виде), а также систем и сетей, в которых она хранится, обрабатывается и передается» [15, с. 130]. Однако различия в концептуальном определении искомого понятия не являются единичными. Разнородности подходов способствует также и различное экономическое положение стран на мировой арене, этому аспекту сопутствуют и вопросы отсутствия единых возможностей в доступе к информационным технологиям. Резюмируя, важно заметить, что вопросы международного регулирования вопросов информационной безопасности сопряжены с целым перечнем проблем, в частности в нормативной сфере, что усложняет осуществление эффективного сотрудничества между странами в обеспечении информационной безопасности, предотвращении информационных войн и информационного терроризма при одновременном обеспечении безопасности информационно-телекоммуникационной инфраструктуры.

Тем не менее, пока существует обозначенный перечень проблем, количество преступлений в информационной сфере неустанно растет, приобретая новые формы своего проявления. Единичные преступления могут носить системный характер. Ярким примером этого является глобальная атака на SolarWinds, произошедшая 13 декабря 2020 года. Ее результатами оказались системные проблемы в информационном обеспечении как министерств Соединенных Штатов Америки, так и крупных компаний частного сектора. Было взломано более 16 000 компьютерных систем. Все, что произошло, является результатом кибератаки на компанию SolarWinds. Чреда подобного рода событий диагностируют проблему того, что международное сообщество не способны к регулированию подобного рода проблем. Анализируя международные документы, статьи, статистику и конкретные события, стоит выделить ключевые проблемы, которые сопряжены со спецификой международной информационной безопасности:

1. Проблема ситуации, при которой информационные ресурсы оказываются в зависимости друг от друга. Подобное положение весьма точно

описывает технология «блокчейна». При возникновении проблем в определенном секторе информационных ресурсов, под угрозу могут попасть смежные ему. Данный аспект сигнализирует о необходимости улучшения уровня кибербезопасности как со стороны государственных структур, так и со стороны сектора НПО.

2. Увеличение числа кибератак и невозможность государства в их урегулировании. К примеру, на данный аспект довольно подробно ссылаются исследователи, участвовавшие в создании доклада Всемирного экономического форума, посвященного проблемам глобального характера. Помимо прочего, в нем постулируется идея отсутствия опыта у государственных структур в регулировании вопросов кибератак, а как следствии вопросов преследования ответственных за них людей.

3. Аспекты, связанные с слабым изучением со стороны научного сообщества, 5-G связи. Отсутствие качественных исследований, связанных с уязвимостью новых технологий приводят к тому, что злоумышленники, пользуясь этими уязвимостями, применяют их в собственных интересах.

4. Как было выяснено нами ранее, вопросы доступности технологий информационного толка разным странам. Менее подготовленные к разным формам кибератак государства становятся ключевыми целями со стороны преступников. Отсутствие солидарного взгляда государств в отношении вопросов обеспечения информационной безопасности связаны с отсутствием закрепленных нормативных правил и действий в отношении к данного рода явлениям. Как следствие, проблемы информационной киберпреступности приобретают спекулятивный характер на международном уровне.

Эта проблема была предметом обсуждения в течение многих лет. Как мы проанализировали выше, на глобальном уровне существует как минимум две концепции информационной международной безопасности, Российская и концепция США. Для решения насущных проблем, определяющих международно-правовое регулирование и сотрудничество государств на

глобальном уровне в информационной сфере, следует пристально относится к осуществлению таких действий, как:

1. Содействие в сотрудничестве государств, национальных структур, организаций коммерческого толка и научных объединений в вопросах обеспечения кибербезопасности.

2. Разработка и следование международных институтов в едином направлении в вопросах определения ключевых проблем в информационной сфере.

3. Создание единого международно-правового акта, являющегося своего рода согласием мнений различных сторон на принципах уважения государственного суверенитета, который включает концептуальный аппарат, цели, задачи, виды угроз, а также положения об ответственности государств в международном информационном пространстве.

4. Осуществление совместных инициатив в области научного изучения вопросов информационной безопасности и обмен опытом различными государствами.

5. Создание эффективного механизма противодействия информационным угрозам на основе единого документа. Создание единых правил, признанных большинством государств, создаст эффективный механизм обеспечения международной информационной безопасности.

Например, в Российской Федерации главным законом об информации является Федеральный закон «Об информации, информационных технологиях и о защите информации» [5]. Он определяет информацию — как любые данные и сведения независимо от формы их представления, определяет критерии конфиденциальной и общедоступной информации. Также есть Федеральный закон «О персональных данных» [4], который обязывает компании сохранять конфиденциальность личных данных пользователей. В каждом государстве есть законы, которые защищают конфиденциальную информацию граждан. Однако на международном уровне вопрос информационной безопасности до сих пор стоит довольно остро.

Следуя ключевым положениям данных нормативно-правовых актов, важно отметить, что они определяют запрет использования коммуникационных структур и технологий в экстремистских и преступных целях. При этом на глобальном уровне данный вопрос требует более тщательной и убедительной артикуляции.

Исходя из опыта взаимодействия государств в сфере обеспечения глобальной информационной безопасности, мы можем выделить перечень возможных решений, способных оказать содействие в преодолении обозначенной глобальной проблемы, среди них:

1. Закрепление единого акта, закрепляющего международные нормы для урегулирования международных ситуаций, и создание единой концепции международной информационной безопасности.

2. Наращивание опыта в киберпространстве. Профилактические меры для программ-кибератак, а именно: определение процента угроз, резервное копирование ИТ-ресурсов и данных, обеспечение непрерывности операций при сбоях в работе компьютерных систем, а также обучение организаций реалистичным киберответам. Обучение дипломированных специалистов в области киберпреступлений, которые смогут в разумные сроки выявлять преступников, а также защищать данные международных организаций и своих стран.

3. Сотрудничество в сфере доказательств и преследования киберпреступников, дабы уменьшить разрыв между государствами. Таким образом, придерживаясь правильного курса в вопросе международной информационной безопасности, мы сможем укрепить безопасность международных организаций, самих стран и, конечно же, граждан, так как в нашем мире всё взаимосвязано.

Глобальный и региональный подход в этой связи предполагает, либо принятие единой системы решения проблем информационной безопасности на международном уровне, либо же совершенствование систем на национальном уровне. Ввиду того, что информационное пространство обладает глобальным

характером, возникает явная необходимость принятия международных мер по обеспечению его безопасности, одновременно и совершенствования механизмов правового регулирования на международном уровне.

На регулирование вопросов международной информационной безопасности направлено внимание многих международных организаций, в число которых входят: Организация Объединенных Наций, Организация Договора о коллективной безопасности, НАТО, а также Шанхайская организация сотрудничества и другие. Деятельность международных организаций предоставляет консультативные механизмы, а также позволяет объединить усилия стран-членов международного сообщества в деле противодействия глобальным и универсальным информационным угрозам [35, с. 125].

Как мы уже отмечали ранее существующие международные соглашения в области вопросов информационной безопасности приобретают скорее набор желаемых действий, носящий рекомендационных характер. При этом отсутствует набор реальных действий по предотвращению ключевых проблем.

Представляется, что отсутствуют комплексные международные договоры универсального характера, направленные на регулирование сотрудничества государств как в сфере обеспечения международной информационной безопасности, так и в борьбе с преступностью [46, с. 78]. То же отмечали С.Б. Мякинина и Н.А. Шеяфетдинова в работе, посвященной проблемам международной кибербезопасности [48, с. 102]. В то же время надлежит обозначить, что в настоящее время существует Конвенция о преступности в сфере компьютерной информации (ETS N 185) [3].

Данный нормативный документ был ратифицирован более пятью десятками государств, в которые вошли все представители Европейского Союза, а также США, Япония, Австралия и Израиль. Однако, Россия не участвует в данной Конвенции. При этом, следует отметить, что международное закрепление вопросов по обеспечению безопасности информационного пространства в большей степени развито на межгосударственном уровне. В

настоящее время прослеживается сотрудничество между государствами в области разрешения вопросов информационной безопасности, которое проявляется в форме международных договоров.

Следуя логике исследователя И.Э. Кванталиани, способствовать регулированию возникающих проблем в сфере информационного взаимодействия стоит, прибегнув к таким мерам, как постоянный обмен информацией о возможных угрозах международной информационной безопасности между государствами, о национальных стратегиях и подходах использования ИКТ в межгосударственных конфликтах, а также о практике обеспечения информационной безопасности [33, с. 146].

Соглашение, приведенное в качестве примера между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области международной информационной безопасности, подписанное 26 мая 2015 года, устанавливает перечень мер, которые ставят под угрозу международную информационную безопасность, и устанавливает, что сотрудничество между Российской Федерацией и правительством Китайской Народной Республики в целях противодействия террористам и террористическим группировкам. другие незаконные объекты являются приоритетом российско-китайского сотрудничества.

Иными словами, создание подобного рода акта связано с весьма осязаемыми процессами, а именно: обменом важной информации в контексте угроз информационной безопасности, а также в осуществлении процессов совместного участия в интеграционных процессах научного толка и в разработке мер по укреплению доверия. Как мы уже не раз отмечали, на межгосударственном, глобальном уровне концепции информационной безопасности, всевозможные резолюции оказываются инертными в юридическом плане. Фрагментарность подобных актов является ключевой проблемой, связанной с отсутствием единообразных и универсальных правил, регулирующих вопросы международной безопасности информационного пространства.

Следовательно, в обозначенных условиях и обстоятельствах очень важно разработать с учетом успешного опыта стран-лидеров целостный кодификационный нормативно-правовой акт, который полноценно охватил бы различные аспекты формирования государственной политики в сфере национальной безопасности с учетом современного развития международных отношений и международного права в данной сфере, а также определил бы конкретный инструментарий ее реализации. Глобальный подход, в связи с этим оказывается более релевантным по отношению к региональному в силу того, что такой документ позволит подвести нормативно-правовую основу под деятельность различных субъектов, в том числе и государства, но в первую очередь человека и гражданина, в сфере обеспечения различных уровней информационной безопасности общества.

# ЗАКЛЮЧЕНИЕ

По результатам проведённого анализа роли международных организаций в обеспечении информационной безопасности государств, можно сделать ряд принципиальных выводов.

**Во-первых**, сотрудничество между государствами в сфере информационной безопасности необходимо, поскольку оно может ограничить деятельность неправительственных субъектов и киберпреступников. Государства могут быть не в состоянии согласовать все условия совместного соглашения о кибербезопасности, но они могут согласовать раздел соглашения, касающийся конкретных видов преступного поведения.

**Во-вторых**, тема международного сотрудничества в вопросах обеспечения международной безопасности вообще и информационной безопасности в частности, стала острой и актуальной в современном мире. Международное сообщество в рамках международных организаций и благодаря механизмам ООН демонстрирует стремление к масштабному сотрудничеству, объединению усилий, взаимодействию, совместному участию, открытости и прозрачности, ответственности и инновационности в решении общей проблемы безопасного мира.

**В-третьих**, предложенный Россией формат открытого диалога по безопасности ИКТ продемонстрировал свою эффективность и актуальность в решении насущных проблем, стоящих перед международным сообществом. Работа ГПЭ помогла повысить доверие и взаимопонимание между государствами, но раскол в позициях не был преодолен полностью, о чем свидетельствуют альтернативные проекты в области сотрудничества по безопасности ИКТ, предложенные западными странами.

**В-четвертых**, существует разница между концепцией кибербезопасности и информационной безопасности. Кроме того, взгляды стран-членов ШОС, БРИКС и ОДКБ идут вразрез с преобладанием североамериканской проекции осуществления контроля над киберпространством. Государства организации

ШОС, БРИКС и ОДКБ стараются проецировать собственное видение в решении вопросов информационной безопасности на интеграционные объединения более высокого порядка, такие как Организация Объединенных Наций, для предложения новых моделей международного законодательства в цифровой сфере.

**В-пятых,** в обозначенных условиях и обстоятельствах очень важно разработать с учетом успешного опыта стран-лидеров целостный кодификационный нормативно-правовой акт, который полноценно охватил бы различные аспекты формирования государственной политики в сфере национальной безопасности с учетом современного развития международных отношений и международного права в данной сфере, а также определил бы конкретный инструментарий ее реализации. Глобальный подход, в связи с этим оказывается более релевантным по отношению к региональному в силу того, что такой документ позволит подвести нормативно-правовую основу под деятельность различных субъектов, в том числе и государства, но в первую очередь человека и гражданина, в сфере обеспечения различных уровней информационной безопасности общества.

Содержание исследуемой проблематики, безусловно, шире и едва ли может быть исчерпано в рамках данного формата исследования. В связи с чем это открывает перспективы для дальнейших исследований.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

**Официальные документы:**

1. Доклад Генерального секретаря ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». – URL: https:// documents-dds-ny. un.org/doc/UNDOC/GEN/N00/535/04/ PDF/N0053504.pdf (дата обращения: 07.04.2023)

2. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН № 53/70 // Организация Объединенных наций [сайт]. 4 декабря 1998. – URL: http://goo.gl/YzdrVG (дата обращения: 07.04.2023).

3. Конвенция о преступности в сфере компьютерной информации (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) (с изм. от 28.01.2003) // СПС Консультант Плюс. URL: http://www.consultant.ru/ (дата обращения 20.041.2023).

4. О персональных данных : Федеральный закон № 152-ФЗ : (редакция от 02.07.2021 года) : принят Гос. Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года // КонсультантПлюс : справочная правовая система. URL: www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 26.04.2023).

5. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ (редакция от 30 декабря 2021 года) : принят Гос. Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года // КонсультантПлюс : справочная правовая система. URL: www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 26.04.2023).

6. Проект Конвенции Организации Объединенных Наций «О сотрудничестве в сфере противодействия информационойпреступности». URL: http://www.mid.ru (дата обращения 11.04.2023).

7. Распоряжение Правительства РФ от 30 апреля 2015 г. N 788-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационнойбезопасности» // СЗ РФ. 2015. N 19, ст. 2859

8. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary General. Document A/54/213. August 10, 1999. – P. 11. – URL: https://disarmamentlibrary.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$ FILE/A-54-213.pdf (дата обращения: 07.04.2023).

9. Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary General. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/65/154&referer=/english/&Lang=R.

10. Group of Governmental Experts on Developments in Information and Telecommunications in the Context of International Security. Note by the Secretary-General, URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/65/201&referer=/english/&Lang=R.

11. Group of Governmental Experts on Advances in Informatization and Telecommunications in the Context of International Security. Note of the Secretary-General. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R.

12. Resolution adopted by the General Assembly on December 27, 2013 [on the report of the First Committee (A / 68/406)]. URL: https://undocs.org/ru/A/RES/68/243.

13. Rules of Conduct in the Field of International Information Security: Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian

Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. A / 66/359. URL: http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf

14. Shanghai Cooperation Organization (SCO). (2009). Agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security. Retrieved July 10th, 2018, from http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

**Монографии и статьи:**

15. Батуева Е.В. Виртуальная реальность: концепция угроз информационной безопасности США и ее международная составляющая// Вестник МГИМО университета. 2014. № 3. С. 130

16. Безкоровайный М.М. Кибербезопасность подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – 2014. – №1 (2) – С. 22-27.

17. Бейсли-Уокер Б., Боммелер К., Международная информационная безопасность и глобальное управление Интернетом: взгляд из Женевы глазами российских и международных экспертов / Б. Бейсли-Уокер, К. Боммелер, В.Л. Васильев, Р. Вебер, В.В. Львович, В.А. Орлов и др. // Индекс безопасности. – 2013. – Т.19. – № 1 (104). – С. 185-205.

18. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества: Научно-популярное / Демидов О. - М.: Альпина Паблишер, 2016. - 198 с

19. Гончаров Д.К., Айдарова Е.М. Экономика упоминаний в информационном обществе // Международный журнал гуманитарных и естественных наук. 2020. № 7-2(46). С. 97-99.

20. Грибков Д.Г. О формировании системы международной информационной безопасности // Международная жизнь. – 2015. – № 8. – С. 86-92.

21. Дубень А.К. Международно-правовые основы обеспечения информационной безопасности: проблемы и приоритеты // Международное право. – 2022. – № 1. – С. 51 - 60.

22. Душкин Р. В. Обзор текущего состояния квантовых технологий. /Р.В.Душкин// Компьютерные исследования и моделирование 2018. – Т. 10. – № 2. – С. 165.

23. Жаглин А. В. Понятийный аппарат теории национальной безопасности/ А.В. Жаглин // Вестник Воронежского института МВД России – 2014. – № 3 – С. 160.

24. Забара И. Н. Деятельность ООН в развитии международно-правового регулирования информационных отношений // Вестник РУДН. Серия Юридические науки. – 2013. – № 1. – С. 136–143.

25. Запечников С.В. Проблемы обеспечения информационной безопасности больших данных / С. В. Запечников, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой // Безопасность информационных технологий. – 2014. – Т. 21. – №. 3. – С. 9

26. Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности. – Вестник МГИМО Университета. – 2016. – № 4. – С. 235-247.

27. Ирошников Д. В. Соотношение понятий "опасность", "угроза", "вызов" и "риск" в правовой доктрине, действующем законодательстве и документах стратегического планирования / Ирошников Д. В. // Транспорт, право и безопасность – 2017. – № 12 – С. 97.

28. Ищейнов В.Я. Информационная безопасность и защита информации: учеб. пособие. Москва: Директ-Медиа, 2020. – 271 с.

29. Калашников А.О. Влияние новых технологий на информационную безопасность критической информационной инфраструктуры/ А.О. Калашников, Е.В. Аникина // Информация и безопасность – 2019. – № 2 – С. 56.

30. Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения – 2017. – № 6 – С. 48

31. Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни / Н.В. Кардава // Каспийский регион: политика, экономика, культура – 2019. – № 3(60). – С. 74

32. Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. д-ра юрид. Наук / М.Б. Касенова. – М., 2016. – С.27.

33. Кванталиани И.Э. Проблемы международно-правового регулирования вопросов информационной безопасности // Право и государство пресс. 2013. № 11 (107). С. 143–146

34. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Отв. ред. М.Б. Касенова; сост. О.В. Демидов, М.Б. Касенова. М.: Статут, 2014. – 464 с.

35. Кириленко В.П., Алексеев Г.В. Международное право иинформационная безопасность государств: монография. СПб., 2016. 394 с.

36. Кларк Р., Найк Р. Третья мировая война. Какой она будет? Высокие технологии на службе милитаризма. С-П., Питер, 2011. С. 56

37. Когаловский М.Р. Глоссарий по информационному обществу / Под общ. ред. Ю. Е. Хохлова. – Москва: Институт развития информационного общества, 2009. – 160 с.

38. Козлова Д.Р., Козлова Н.Ш. Информационная безопасность в виртуальной среде // Наука и творчество: вклад молодежи: материалы Всерос. молодеж. науч.-практ. конф. студентов, аспирантов и молодых ученых. Махачкала, 2020. – С. 48–50.

39. Косотина М.А. Проблемы становления нового мирового порядка. 2019. - № 5. - С. 82-86.

40. Крутских А.В. Глобальная киберповестка: дипломатическая победа // Международная жизнь. – 2021. – № 7. – С. 1-11.

41. Кучерявый М.М. Глобальное информационное общество и проблемы безопасности // Власть. – 2013. – № 9. – С. 89–92.

42. Манойло А.В. Методологические основы формирования единого пространства коллективной безопасности ШОС и БРИКС в информационной сфере (Устный) Международный научно-практический форум «Россия в XXI веке: глобальные вызовы, риски и решения», Москва, Российская академия наук, Россия, 5-6 июня 2019. С.100-106

43. Маслакова Е.А. К вопросу о международном сотруд- ничестве в сфере обеспечения информационной безопасности / Маслакова Е.А., Жилкин М.Г., Кача- лов В.В. // Вестник Московского университетата МВД России. – 2015. – № 9. – С. 75–7

44. Международная информационная безопасность в трех томах. Том 1: Учебник для вузов / под общ ред. А.В. Крутских. М.: Издательство «Аспект-Пресс», 2019. – 384 с.

45. Мельникова О.А. Средства и методы обеспечения информационного сопровождения внешней политики государства // Международная жизнь. – 2017. – № 5. – С. 155–168.

46. Мороз Н.О. Международно-правовые основы обеспечения международной информационной безопасности // Труд. Профсоюзы. Общество. 2016. № 1 (51). С. 77–81

47. Мурзин Ф.А. Облачные технологии: основные понятия, задачи и тенденции развития / Ф.А.Мурзин, Т.В. Батура, Д.Ф Семич. // Программные продукты, системы и алгоритмы. – 2014. – № 1. – С. 64.

48. Мякинина С.Б., Шеяфетдинова Н.А. Проблемы международной кибербезопасности // Современное право. 2020. № 5. С.100–104.

49. Полякова Т.А. Развитие системы международной информационной безопасности и стратегические задачи правового обеспечения информационной безопасности на национальном и региональных уровнях // Сборник докладов участников пятнадцатого международного форума «Партнерство государства,

бизнеса и гражданского общества при обеспечении международной информационной безопасности» 27-29 сентября 2021 г., М., 2021. – С. 47-50.

50. Полякова Т.А. Теоретико-методологические проблемы цифровизации и трансформация информационного права // Третьи Бачиловские чтения. Цифровая трансформация: вызовы праву и векторы научных исследований: материалы Международной научно-практической конференции / под общ. ред. А.Н. Савенкова; отв. ред. Т.А. Полякова, А.В. Минбалеева. М., 2020. – 312 с

51. Потапов А.С. Технологии искусственного интеллекта /А.С. Потапов – СПб: СПбГУ ИТМО, 2010. С.3

52. Смирнов. А.И. Современные информационные технологии в международных отношениях. М., МГИМО Университет, 2017. С. 26

53. Цветков В.Я. Кибер физические системы /В.Я. Цветков// Международный журнал прикладных и фундаментальных исследований. – 2017. – № 6-1. – С. 64

54. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» ; ИНФРА-М, 2016. — 416 с.

55. Buzan B., Wæver O., De Wilde J. 1998. Security: a New Framework for Analysis. Lynne Rienner Publishers. 239 p.

56. Kerschischnig G. Cyberthreats and International Law. / G. Kerschischnig - The Hague, 2012. - P. 5.

**Интернет-ресурсы:**

57. Вызовы информационной безопасности и опыт ОДКБ. 2-я Международная конференция «Инфофорум-Югра» // Международная жизнь [Электронный ресурс]. – Режим доступа: https://interaffairs.ru/news/show/20062 (дата обращения 25.04.2023)

58. Boyko, S. M., “Problems of International Information Security at the SCO and BRICS Sites,” URL: https://www.nkibrics.ru/posts/show/5c504e2f6272697aca810000. (дата обращения 17.04.2023)

59. ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. – URL: https://www.iso.org/ru/standard/44375.html (дата обращения 17.04.2023)

60. Nato’s Warsaw summit is a test the west must pass. URL: www.ft.com/content/f36c7b2a-3f7d-11e6-9f2c (дата обращения 17.04.2023)

61. The 25 Largest Internet Companies In The World URL: www.worldatlas.com/articles/ (дата обращения 17.04.2023)

62. Towards a secure cyberspace via regional cooperation. URL: https://dig.watch/processes/ungge (дата обращения 17.04.2023)

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
«06» 09 2023 г.

# БАКАЛАВРСКАЯ РАБОТА

41.03.05. Международные отношения

Роль международных организаций в обеспечении информационной безопасности государств

Руководитель 10.05.2023 доцент, к.ю.н В.А. Мещериков
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник 10.05.2023 А.А. Пахомчик
подпись, дата инициалы, фамилия

Красноярск 2023