Роль ООН в обеспечении международной информационной безопасности

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....3

ГЛАВА 1. МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.....6

1.1. Определение понятия международной информационной безопасности.....6

1.2. Актуальные угрозы и вызовы международной информационной безопасности.....8

1.3. Объекты и субъекты международной информационной безопасности.....11

ГЛАВА 2. ДЕЯТЕЛЬНОСТЬ ООН ПО ОБЕСПЕЧЕНИЮ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....14

2.1. Политика и инициативы ООН в области международной информационной безопасности.....14

2.2. Роль геополитической напряженности в препятствовании усилиям ООН в области информационной безопасности.....18

2.3. Оценка эффективности подхода ООН к обеспечению информационной безопасности.....20

ЗАКЛЮЧЕНИЕ.....23

ВВЕДЕНИЕ

Информационная безопасность является одной из ключевых проблем в современном мире. Быстрый рост информационных технологий и их все более широкое использование создают новые возможности и вызовы для международной общности. В связи с этим, вопросы международной информационной безопасности становятся все более актуальными и требуют внимания со стороны государств, международных организаций и общественности. Информация — один из показателей превосходства страны над конкурентами. Борьба, которая ведётся за обладание информацией, достижение и удержание информационного превосходства занимает значительное место в конкуренции между странами-лидерами экономического развития.[1]

Роль ООН в обеспечении международной информационной безопасности является *крайне важной и актуальной* в современном мире, где киберугрозы становятся все более серьезными и распространенными. С развитием технологий и расширением доступа к интернету, международная информационная безопасность становится все более важной. ООН принимает меры для борьбы с киберугрозами и защиты международной информационной безопасности. Например, в 2015 году была создана Группа правительственных экспертов по кибербезопасности (GGE), которая занимается разработкой рекомендаций по обеспечению безопасности в киберпространстве. Кроме того, ООН проводит обучающие мероприятия и различные формы консультации для государств и организаций по вопросам информационной безопасности.

Цель данной работы — проанализировать роль ООН в обеспечении международной информационно безопасности.

---

[1] Батуева Е. В. Информационные войны США: К определению национальной киберстратегии // Международные процессы. 2014. Т. 12. No 1–2. С. 117–127. [Электронный ресурс]. — Режим доступа: http://www.intertrends.ru/old/thirty-seventh/Batueva.pdf (дата обращения: 12.05.2023)

Для достижения цели были поставлены *задачи*:

- исследование международных источников, таких как официальные документы международных организаций и союзов, учебная и научная литература, диссертации, статьи из журналов и сборников, посвященных проблемам международной информационной безопасности;
- анализ основных тенденций, подходов и вызовов в области международной информационной безопасности;
- оценка роли и ответственности ООН в обеспечении безопасного и устойчивого киберпространства.

Объектом исследования является деятельность ООН по обеспечению международной информационной безопасности.

Предметом исследования являются меры, которые ООН принимает для борьбы с киберугрозами и защиты международной информационной безопасности, включая создание и развитие соответствующих структур и механизмов, проведение обучающих мероприятий и консультаций, а также разработку рекомендаций по обеспечению безопасности в киберпространстве.

Нормативной базой работы являются официальные документы Организации Объединенных Наций, такие как резолюции Генеральной Ассамблеи, которые оказывают влияние на разработку и принятие международных норм и правил в области информационной безопасности. Также в работе будут рассмотрены руководящие принципы и документы других международных организаций, таких как Международный союз связи (ITU), Европейская комиссия (ЕС) и другие. Будет проанализирована актуальная учебная и научная литература, включая книги, статьи и научные исследования, относящиеся к международной информационной безопасности.

В рамках *теоретической основы* работы будут проанализированы учебная и научная литература, включая книги и статьи, которые предлагают теоретические и практические подходы к решению проблем международной информационной безопасности. Диссертации и научные статьи также помогут раскрыть актуальные исследования в данной области.

Степень научной разработанности проблемы преступлений в информационной сфере и безопасности этой сферы в целом достаточно велика. Свои научные работы — статьи и диссертации — на эту тему представили Бриллиантов А. В., Векленко В. В., Гаврилов Б. Я., Горелик И. Б., Зиновьева Е. С., Кривогин М. С., Кругликов Л. Л., Ляпунов Ю. И., Русскевич Е. А., Талипов Л. Р., Тропина Т. Л., Яцеленко Б. В. и другие научные деятели.

Методологическая основа работы включает в себя различные методы исследования. Для получения информации были использованы поисковый, аналитический и аналогический методы исследования. Для осуществления поискового метода были использованы учебная и публицистическая литература, правовые документы, находящиеся в открытом доступе, информация, полученная из интернета, а также данные проведённого анализа.

Важной частью работы будет анализ роли и ответственности государств и международных организаций в обеспечении безопасного и устойчивого киберпространства. Будут рассмотрены международные инициативы, договоры и соглашения, направленные на сотрудничество и координацию действий в области информационной безопасности. В работе будет также рассмотрена проблема баланса между обеспечением безопасности и защитой приватности, а также вопросы кибервойны и кибердипломатии.

Результаты исследования предоставят полное представление о состоянии и развитии международной информационной безопасности, а также выявят основные вызовы и перспективы в этой области. Это позволит сформулировать рекомендации и предложения для дальнейших действий и усовершенствования международных подходов к обеспечению информационной безопасности.

Структура работы представляет собой введение, основную часть, состоящую из двух глав, заключение и список использованных источников. Во введении обозначены основные аспекты работы, в первой главе представлена теоретическая информация, вторая глава является аналитической. В заключении представлены основные выводы работы.

ГЛАВА 1. МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Определение понятия международной информационной безопасности

Международная информационная безопасность является важной и сложной областью, требующей четкого определения и понимания. В данном разделе будет проведен анализ различных подходов и определений, предложенных различными организациями и авторами в рамках международной общности.

Международная информационная безопасность может быть определена как состояние защищенности информационных ресурсов, систем и данных от угроз и рисков на международном уровне. Это включает в себя не только защиту конфиденциальности, целостности и доступности информации, но и противодействие киберпреступности, кибервойне, а также обеспечение устойчивости и безопасности киберпространства.

Однако, несмотря на общепринятое определение, существуют различные интерпретации и подходы к понятию международной информационной безопасности. Определения могут отличаться в зависимости от контекста, организации или стратегических приоритетов. Рассмотрим некоторые из них.

Организация Объединенных Наций (ООН) рассматривает международную информационную безопасность в контексте устойчивого развития и международной стабильности. Согласно доктрине ООН, информационная безопасность включает в себя защиту информационных систем от незаконного доступа, вмешательства и уничтожения, а также противодействие киберпреступности и защиту прав человека в киберпространстве.

Другие организации, такие как Международный Телекоммуникационный Союз (МТС) и Организация экономического сотрудничества и развития (ОЭСР), в своих определениях акцентируют

внимание на технических аспектах информационной безопасности, таких как защита от кибератак и обеспечение безопасности информационных инфраструктур.

Кроме официальных организаций, авторы и исследователи также вносят свой вклад в определение понятия международной информационной безопасности. Например, Майкл Нил из Университета Оксфорд определяет международную информационную безопасность как "состояние, при котором международные акторы обладают доверием в отношении сохранности информации и информационных систем в международном пространстве, а также способностью действовать в нем без опасения от угроз и рисков, связанных с информацией".

Важным аспектом определения международной информационной безопасности является учет многообразия угроз и рисков, с которыми сталкиваются государства и международные организации. Это могут быть кибератаки, хакерские атаки, вирусы и вредоносное программное обеспечение, кибершпионаж, дезинформация и манипуляция информацией, а также угрозы приватности и нарушение прав человека в киберпространстве. При определении международной информационной безопасности необходимо учитывать как традиционные, так и новые формы угроз, возникающие в связи с развитием информационных технологий.

В эпоху трансформации и динамического развития мира вокруг нас информационная инфраструктура создаёт впечатляющее количество преимуществ для обычного человека. Развитие информационной инфраструктуры увеличивает качество, скорость и доступность различного вида услуг, начиная финансовыми услугами и заканчиваю доставкой продуктов к двери. С наступлением интенсивной информатизации общества меняется привычная инфраструктура экономической деятельности, приоритет отдается цифровым технологиям (электронная экономика).[2] Бизнес-процессы

[2] Листопад М. Е., Коротченко С. Е. // National Interests: Priorities and Security, 2017, vol. 13, iss. 6, pp. 1162–1175. ISSN 2311-875X (дата обращения: 12.05.2023)

автоматизируются с помощью информационных систем и интернет-технологий (электронный бизнес), коммерческие транзакции осуществляются при помощи специализированных информационных технологий (электронная коммерция), что влияет на развитие электронных денег, электронной торговли, электронного маркетинга, электронного банкинга, электронных страховых услуг.[3] Но вместе с динамичным развитием инфраструктуры возникают и совершенно новые риски, которые грамотная государственная политика должна предусмотреть при разработки концепции или стратегии развития государства на краткосрочный и долгосрочный периоды.

Как было обозначено в предыдущем параграфе, цифровизация влечет за собой разноплановые тенденции, которые носят объективный характер.[4] Избежать их невозможно, но важность событий очевидна, особенно учитывая развитие нового технологического уклада во всем развитом мире.

Также важно отметить, что понятие международной информационной безопасности включает не только аспекты технической защиты, но и широкий спектр политических, правовых, экономических и социальных аспектов. Это связано с тем, что информационная безопасность является комплексной и междисциплинарной областью, требующей сотрудничества и координации между государствами, международными организациями, частным сектором и гражданским обществом.

1.2. Актуальные угрозы и вызовы международной информационной безопасности

В современном мире международная информационная безопасность сталкивается с рядом актуальных угроз и вызовов, которые требуют особого внимания и дальнейшего исследования. В данном разделе будет проведен

---

[3] Брандман Э.М. Глобализация и информационная безопасность общества // Философия и общество. 2006. No 1. С. 31–41. (дата обращения: 12.05.2023)

[4] Архипова Л. С., Мельникова Д. М. // Оценка современных барьеров, влияющих на цифровизацию российского рынка труда// Региональная экономика и управление: электронный научный журнал. ISSN 1999–2645. — № 2 (70). Режим доступа: https://eee-region.ru/article/7002/ (дата обращения: 12.05.2023)

обзор основных угроз и вызовов, с которыми сталкиваются государства и международные организации в контексте информационной безопасности.

В XXI веке на развитие стран наибольшее влияние оказывают процессы глобализации и цифровизации. В экономически развитых странах набирает обороты новый технологический уклад, в котором роль цифровой экономики становится определяющей.[5]

В Отчете Всемирного экономического форума по глобальным рискам за 2020 кибератаки определены как разновидность базового глобального технологического риска.[6] В качестве мирового тренда отмечается увеличение финансовых потерь от кибератак, нарушение целостности и непрерывности функционирования в том числе финансового рынка (17% всего объема кибератак приходится на финансовый сектор). Изощренность методов, способов и средств совершения кибератак требует от регуляторов гибкости, оперативности, использования инновационных цифровых технологий и методов работы. Соединенные Штаты Америки, Канада, Сингапур, Австралия, Малайзия, Новая Зеландия, Япония, Великобритания, Австрия – эти страны, в большей степени подготовленные к кибератакам, что является фактором ускорения их экономического развития.

Одной из главных угроз в сфере международной информационной безопасности является киберпреступность. Киберпреступные действия, такие как хакерские атаки, фишинг, кибервымогательство и кража личных данных, имеют серьезные последствия для государств и отдельных лиц. Киберпреступники постоянно совершенствуют свои методы и используют новейшие технологии, что создает сложности для их обнаружения и пресечения.

---

[5] Архипова Л. С., Мельникова Д. М. // Оценка современных барьеров, влияющих на цифровизацию российского рынка труда// Региональная экономика и управление: электронный научный журнал. ISSN 1999–2645. — № 2 (70). Режим доступа: https://eee-region.ru/article/7002/ (дата обращения: 12.05.2023)

[6] Отчет Всемирного экономического форума по глобальным рискам за 2020 год // ВЭФ // [Электронный ресурс]. — Режим доступа: https://www.weforum.org/reports/the-global-risks-report-2020/ (дата обращения: 12.05.2023)

Важной угрозой является также кибершпионаж, который может быть осуществлен как государственными, так и негосударственными акторами. Кибершпионы стремятся получить доступ к чувствительной информации, включая коммерческие секреты, военные технологии и государственные секреты. Это создает реальные риски для национальной безопасности и экономического развития государств.

С развитием интернета и социальных сетей возникли новые вызовы для информационной безопасности. Дезинформация, фейковые новости и манипуляции информацией стали мощным инструментом воздействия на общественное мнение и политические процессы. Это влияет на стабильность государств, международные отношения и доверие между странами.

Еще одной актуальной угрозой является кибертерроризм. Террористические группировки могут использовать киберпространство для планирования и совершения террористических актов, в том числе атак на критическую информационную инфраструктуру и коммуникационные сети. Такие атаки могут привести к парализации важных систем и инфраструктур, таких как энергетические сети, транспортные системы и финансовые учреждения.

Помимо этого, нарастает угроза киберразведки со стороны государственных акторов. Государства могут использовать киберспособности для сбора разведывательной информации, включая военные и политические секреты, а также для проведения кибершпионажа с целью вмешательства во внутренние дела других стран.

Еще одним вызовом является защита критической информационной инфраструктуры, такой как системы энергетики, телекоммуникаций и финансов. Атаки на такие системы могут иметь катастрофические последствия для функционирования общества и государства в целом.

Возникающие технологические тренды также представляют угрозу для международной информационной безопасности. Например, Интернет вещей (IoT) и искусственный интеллект (ИИ) создают новые возможности для атак

и злоупотребления информацией. Уязвимости в смарт-устройствах и автоматизированных системах могут быть эксплуатированы злоумышленниками для нанесения ущерба и нарушения приватности.

В свете этих угроз и вызовов, международное сообщество стремится развивать стратегии и меры по защите информационной безопасности. Это включает укрепление правовой базы и международного сотрудничества, создание киберзащитных политик и стандартов, а также повышение осведомленности и компетентности в области информационной безопасности.

1.3. Объекты и субъекты международной информационной безопасности

В международной информационной безопасности существуют различные объекты и субъекты, которые играют важную роль в обеспечении безопасности информационного пространства. В данном разделе будет проведен анализ основных объектов и субъектов международной информационной безопасности, их роли и ответственности.

Объекты международной информационной безопасности представляют собой те элементы информационного пространства, которые нуждаются в защите от угроз и рисков. Включение различных объектов в категорию "объекты международной информационной безопасности" может зависеть от контекста и задач исследования.

Стоит рассмотреть некоторые из основных объектов, которые обычно определяются в рамках международной информационной безопасности:

- *Информационные системы и сети:* включают компьютерные системы, сети связи и другие технические средства, которые обрабатывают, хранят и передают информацию. Защита информационных систем и сетей является важным аспектом обеспечения международной информационной безопасности;
- *Информационные ресурсы и данные:* включает в себя различные формы информации, включая конфиденциальные данные, коммерческие секреты, государственные документы и персональные данные. Защита

информационных ресурсов и данных от несанкционированного доступа, использования и уничтожения является важной задачей;

- *Критическая информационная инфраструктура:* включает системы и объекты, которые критически важны для функционирования государства и общества, такие как энергетические сети, транспортные системы, финансовые учреждения и системы здравоохранения. Защита критической информационной инфраструктуры от атак и сбоев является важным аспектом обеспечения безопасности;
- *Права и свободы в киберпространстве:* обеспечение защиты прав и свобод людей в киберпространстве является одним из ключевых объектов международной информационной безопасности. Включает в себя защиту прав на приватность, свободу слова, доступ к информации и другие связанные права.

Субъекты международной информационной безопасности представляют собой акторов, участвующих в обеспечении безопасности информационного пространства. Они могут быть государствами, международными организациями, частными компаниями, некоммерческими организациями и индивидуальными пользователями.

Рассмотрим некоторые из *основных субъектов* международной информационной безопасности:

- *Государства:* государства играют важную роль в обеспечении международной информационной безопасности. Они разрабатывают политику и законы в области информационной безопасности, осуществляют контроль за киберпространством, защищают критическую информационную инфраструктуру и участвуют в международном сотрудничестве;
- *Международные организации:* организации, такие как ООН, Международный союз электросвязи (МСЭ), Интерпол и другие, имеют значимую роль в координации и сотрудничестве в области информационной безопасности между государствами. Они разрабатывают стандарты,

руководства и проводят тренинги для укрепления информационной безопасности;

- *Частные компании:* Крупные технологические компании, провайдеры интернет-услуг и другие частные организации играют важную роль в защите информационных систем и сетей. Они разрабатывают и внедряют технические меры безопасности, предоставляют услуги по обнаружению и предотвращению кибератак, и участвуют в исследованиях и разработках в области информационной безопасности;
- *Некоммерческие организации и активисты:* различные неправительственные организации, активисты и эксперты также вносят вклад в обеспечении международной информационной безопасности. Они занимаются исследованиями, разработкой стандартов и нормативных документов, проводят обучающие программы и информационные кампании для повышения осведомленности о безопасности в киберпространстве;
- *Индивидуальные пользователи:* пользователи информационных систем и сетей также являются субъектами международной информационной безопасности. Они должны соблюдать меры безопасности, такие как использование надежных паролей, защиту своих устройств от вредоносных программ и быть внимательными при обращении с личной информацией. Кроме того, пользователи должны быть осведомлены о своих правах и ответственностях в киберпространстве.

Взаимодействие между объектами и субъектами международной информационной безопасности является важным аспектом обеспечения безопасности информационного пространства. Государства, международные организации, частные компании, некоммерческие организации и индивидуальные пользователи должны сотрудничать и принимать совместные усилия для предотвращения угроз и рисков в киберпространстве, защиты информационных ресурсов и обеспечения прав и свобод людей в онлайн-среде.

ГЛАВА 2. ДЕЯТЕЛЬНОСТЬ ООН ПО ОБЕСПЕЧЕНИЮ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Политика и инициативы ООН в области международной информационной безопасности

Организация Объединенных Наций (ООН) играет важную роль в разработке политики и инициатив в области международной информационной безопасности. ООН стремится содействовать сотрудничеству государств и координации международных усилий для обеспечения безопасности информационного пространства. В данном разделе будут рассмотрены основные политические документы и инициативы ООН, направленные на международную информационную безопасность.

Генеральная Ассамблея ООН принимает резолюции, которые оказывают влияние на политику и действия государств в области информационной безопасности. Некоторые из ключевых резолюций включают:

Резолюция ООН 55/63 "Меры по предотвращению использования информационных технологий в целях, противоречащих международной безопасности" призывает государства сотрудничать в предотвращении незаконного использования информационных технологий и кибератак, которые противоречат международной безопасности.

Резолюция ООН 70/237 "Повышение безопасности и доверия в использовании информационных и коммуникационных технологий в целях международного мира и безопасности" призывает государства сотрудничать в предотвращении конфликтов в киберпространстве и развитии мер доверия и прозрачности в использовании информационных и коммуникационных технологий.

2.1.2 ООН также создала Группу по экспертам по международной информационной безопасности (ГЭМИБ), которая занимается исследованием и консультированием в области информационной безопасности. ГЭМИБ

проводит анализ современных угроз и вызовов, разрабатывает рекомендации и предлагает меры для обеспечения международной информационной безопасности.[7]

ООН разработала Кибернетическую стратегию, которая определяет приоритеты и принципы действий Организации в области международной информационной безопасности. Стратегия подразумевает создание международной системы, основанной на сотрудничестве и доверии, а также включает в себя укрепление кибер-способностей и приверженность правам человека в киберпространстве.[8]

Форум ООН по глобальной киберпространственной политике является платформой для диалога между государствами, частным сектором, гражданским обществом и академическим сообществом относительно вопросов информационной безопасности. Форум способствует обмену мнениями и опытом, а также обсуждению ключевых тем, включая кибернетическую дипломатию, кибер-гигиену и кибер-законодательство.[9]

ООН активно сотрудничает с другими международными организациями, такими как Международный союз электросвязи (МСЭ), для координации усилий в области международной информационной безопасности. ООН и МСЭ сотрудничают в разработке стандартов и руководств по кибербезопасности, проводят совместные мероприятия и обмен опытом, чтобы повысить информационную безопасность на международном уровне.[10]

---

[7] United Nations Office at Geneva, "Group of Governmental Experts on Advancing responsible state behavior in cyberspace in the context of international security" [Электронный ресурс]. — Режим доступа: https://usun.usmission.gov/remarks-to-the-un-group-of-governmental-experts-on-advancing-responsible-state-behavior-in-cyberspace-in-the-context-of-international-security/ (дата обращения: 12.05.2023)

[8] United Nations, "The United Nations Office of Information and Communications Technology Cybersecurity Strategy for the United Nations System" [Электронный ресурс]. — Режим доступа: https://unite.un.org/ (дата обращения: 12.05.2023)

[9] United Nations, "UN Cyber Policy Forums" [Электронный ресурс]. — Режим доступа: https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf (дата обращения: 12.05.2023)

[10] International Telecommunication Union, "ITU and Cybersecurity" [Электронный ресурс]. — Режим доступа: https://www.unodc.org/roseap/uploads/archive/documents/2011/09/cybercrime-workshop/ppt/Ashish_ITU_Cybersecurity_General_an_f1.pdf (дата обращения: 12.05.2023)

ООН проводит работы по развитию правового режима в области международной информационной безопасности. Принятие международных договоров и соглашений способствует установлению общепризнанных норм и правил поведения государств в киберпространстве. Примером такого правового документа является Группа по международной работе по повышению безопасности в киберпространстве, которая разрабатывает правовые руководства и рекомендации для государств по укреплению международной информационной безопасности.[11]

ООН также активно развивает механизмы технической поддержки в области международной информационной безопасности. Это включает обучение и содействие развитию киберспециалистов в различных странах, предоставление экспертной помощи в оценке уязвимостей и разработке киберзащитных стратегий. Кроме того, ООН оказывает техническую поддержку странам в развитии сетевой инфраструктуры и национальных киберполитик.[12]

ООН осуществляет инициативы по повышению осведомленности и образования в области международной информационной безопасности. Это включает проведение кампаний, образовательных программ и тренингов для широкой аудитории. ООН придает большое значение повышению осведомленности о киберугрозах и способствует образованию в области кибербезопасности. Организация разрабатывает информационные материалы, проводит семинары и конференции, а также поддерживает сети экспертов и партнерство с академическими учреждениями для распространения знаний о международной информационной безопасности.

ООН активно содействует развитию международных стандартов и норм в области международной информационной безопасности. Организация поддерживает работу международных форумов и органов, таких как

---

[11] United Nations General Assembly, "Advancing responsible State behavior in cyberspace in the context of international security" [Электронный ресурс]. — Режим доступа: https://unite.un.org/ (дата обращения: 12.05.2023)

[12] United Nations, "Capacity Development on Cybersecurity" [Электронный ресурс]. — Режим доступа: https://www.itu.int/epublications/ (дата обращения: 12.05.2023)

Международная организация по стандартизации (ISO) и Международный электротехнический комитет (IEC), по созданию и продвижению стандартов в кибербезопасности. ООН также поддерживает разработку и принятие нормативных документов, например, в рамках Группы по повышению безопасности в киберпространстве, с целью обеспечения устойчивого и безопасного функционирования информационных систем.[13]

ООН признает важность трансграничного сотрудничества в области международной информационной безопасности. Организация поддерживает укрепление сотрудничества между государствами, правоохранительными органами и другими заинтересованными сторонами для обмена информацией, обнаружения и расследования киберпреступлений, а также для улучшения реагирования на кибер-инциденты. ООН также стимулирует создание международных механизмов сотрудничества, таких как Совет по безопасности ООН, для обеспечения международной безопасности в киберпространстве.

ООН придает особое значение защите прав человека в киберпространстве. Организация разрабатывает и поддерживает принципы, которые обеспечивают уважение к приватности, свободе выражения и свободному доступу к информации в интернете. ООН также рекомендует государствам разрабатывать и применять политики и законодательство, которые соблюдают права человека в киберпространстве и предотвращают применение киберинструментов для нарушения прав человека.[14]

ООН активно сотрудничает с региональными и международными организациями в области международной информационной безопасности. Организация поддерживает согласование действий и обмен опытом с такими организациями, как Европейский союз, Организация по безопасности и сотрудничеству в Европе (ОБСЕ) и Африканский союз, с целью совместного

---

[13] International Telecommunication Union, "ITU and Cybersecurity Standards" [Электронный ресурс]. — Режим доступа: https://www.itu/ (дата обращения: 12.05.2023)

[14] United Nations Human Rights Council, "The Right to Privacy in the Digital Age" [Электронный ресурс]. — Режим доступа: https://ifap.ru/pr/2021/n210920a.pdf (дата обращения: 12.05.2023)

решения проблем информационной безопасности и укрепления глобального киберпространства.

2.2. Роль геополитической напряженности в препятствовании усилиям ООН в области информационной безопасности

Геополитическая напряженность играет значительную роль в препятствовании усилиям ООН в области информационной безопасности. Сложные политические отношения и конфликты между государствами могут стать препятствием для развития сотрудничества и достижения консенсуса в вопросах информационной безопасности.

Геополитическая напряженность играет существенную роль в препятствовании усилиям ООН в области информационной безопасности. Согласно теории политического реализма, государства стремятся к власти и выживанию, что создает конкуренцию и конфликты в международной системе. Эти геополитические напряжения могут негативно сказываться на развитии сотрудничества и достижении консенсуса в вопросах информационной безопасности.

Стоит выделить основные проявления препятствий в развитии сотрудничества между государствами в рамках обеспечения информационной безопасности[15]:

- Ограничение доступа к информации: во время геополитических конфликтов государства могут ограничивать доступ к информации и проводить цензуру в цифровом пространстве. Это может привести к нарушению свободы выражения, свободного доступа к информации и ограничению прав человека в киберпространстве;
- Несогласие с международными нормами: государства могут не соглашаться с международными нормами и стандартами в области информационной безопасности, предлагаемыми ООН. Различия в

[15] United Nations Human Rights Council, "The Right to Privacy in the Digital Age" [Электронный ресурс]. — Режим доступа: https://ifap.ru/pr/2021/n210920a.pdf (дата обращения: 12.05.2023)

геополитических интересах и политических системах могут создавать разногласия и затруднять достижение соглашений по вопросам кибербезопасности;

- Кибероперации и кибервойны: геополитические конфликты могут приводить к нарастанию кибероперациий и кибервойн. Государства могут использовать киберинструменты для осуществления шпионажа, кибератак и дестабилизации информационных систем других государств[16]. Это создает повышенные угрозы для информационной безопасности и усложняет усилия ООН по обеспечению киберстабильности;
- Политическая блокировка и взаимное недоверие: геополитическая напряженность может приводить к политической блокировке и взаимному недоверию между государствами. Это может затруднить усилия ООН по сотрудничеству в области информационной безопасности. Возможность проведения конструктивного диалога и достижения согласия по вопросам кибербезопасности становится маловероятной при наличии геополитических конфликтов и напряженных отношений между странами;
- Пропаганда и дезинформация: геополитическая напряженность может способствовать распространению пропаганды и дезинформации в цифровом пространстве. Государства могут использовать информационные технологии для манипулирования общественным мнением, внедрения вредоносного контента и подрыва доверия к информационным системам других государств. Это создает угрозы для информационной безопасности и затрудняет деятельность ООН по противодействию дезинформации и защите от киберманипуляций;
- Формирование блоков интересов: геополитическая напряженность может способствовать формированию блоков интересов в области информационной безопасности. Государства могут объединяться на основе

[16] Зиновьева, Е. С. Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества / Е. С. Зиновьева; Московский государственный институт международных отношений (Университет) МИД России. – Москва: МГИМО-Университет, 2021. – 282 с.: ил., табл. – Режим доступа – https://biblioclub.ru/index.php?page=book&id=619899 (дата обращения: 12.05.2023)

геополитических факторов и формировать альянсы, которые преследуют собственные цели и интересы в киберпространстве.[17] Это может привести к разделению и конкуренции в области разработки международных норм и стандартов информационной безопасности, что затрудняет усилия ООН по обеспечению единого и согласованного подхода;

- Нарушение кибердоверия: геополитическая напряженность может привести к нарушению кибердоверия между государствами. Подозрения в кибершпионаже, кибератаках и нарушениях информационной безопасности могут привести к взаимным обвинениям и усилением конфликтов, что усложняет усилия ООН по содействию сотрудничеству в области информационной безопасности.

Таким образом, геополитическая напряженность оказывает отрицательное влияние на усилия ООН в области информационной безопасности. Ограничение доступа к информации, несогласие с международными нормами, нарастание кибероперациий, политическая блокировка, распространение пропаганды и формирование блоков интересов создают сложности для достижения консенсуса и эффективного сотрудничества в решении вопросов кибербезопасности. Разработка стратегий по преодолению геополитических разногласий и налаживание конструктивного диалога между государствами являются важными шагами в направлении улучшения информационной безопасности под эгидой ООН.

2.3. Оценка эффективности подхода ООН к обеспечению информационной безопасности

Оценка эффективности подхода ООН к обеспечению информационной безопасности является важным аспектом в понимании эффективности деятельности организации в этой области. Проведение такой оценки позволяет

[17] World Economic Forum, "Competing Cyber Norms: A Global Conflict in the Making?" [Электронный ресурс]. — Режим доступа: https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23/ (дата обращения: 12.05.2023)

выявить достижения, проблемы и потенциальные области улучшений в работе ООН по обеспечению международной информационной безопасности.

Оценка соблюдения международных норм и стандартов: Важным критерием оценки эффективности подхода ООН является соблюдение международных норм и стандартов в области информационной безопасности. Оценка должна учитывать, насколько государства следуют принципам и рекомендациям ООН, таким как "Таллинская руководящая принципы в области национальной политики в киберпространстве" и "Киберстабильность".[18]

Сотрудничество с другими международными организациями: Оценка эффективности подхода ООН также требует учета уровня сотрудничества с другими международными организациями, такими как Международный союз телекоммуникаций (МСТ) и Международный союз электросвязи (ITU). Взаимодействие и координация усилий между ООН и другими организациями могут способствовать эффективному решению проблем информационной безопасности.

Вовлечение государств и стейкхолдеров: Оценка эффективности подхода ООН также должна учитывать степень вовлечения государств и других заинтересованных сторон в процессы принятия решений и разработки политики в области информационной безопасности. Важно оценить, насколько эти стейкхолдеры активно участвуют в формировании и реализации стратегий и программ ООН в данной области и насколько их интересы и потребности учитываются. В частности, оценка должна обратить внимание на вовлечение частных компаний, гражданского общества и академического сообщества в диалог с ООН по вопросам информационной безопасности.

Анализ результатов программ и проектов: Эффективность подхода ООН может быть измерена через анализ результатов программ и проектов, реализуемых в области информационной безопасности. Оценка должна

---

[18] Бойко, С.М. Международная информационная безопасность: новые вызовы и угрозы / Сергей Михайлович Бойко. – Текст: электронный // Международная жизнь. – 2022. №11. [Электронный ресурс]. — Режим доступа: https://interaffairs.ru/jauthor/material/2738 (дата обращения: 12.05.2023)

учитывать степень достижения поставленных целей, а также оценку эффективности использования ресурсов и мер управления рисками.

Механизмы мониторинга и отчетности: Оценка эффективности подхода ООН к обеспечению информационной безопасности требует оценки существующих механизмов мониторинга и отчетности. Важно определить, насколько системы сбора данных и отчетности позволяют анализировать и оценивать состояние информационной безопасности, а также оценивать прогресс и достижения в этой области.

В заключение следует отметить, что оценка эффективности подхода ООН к обеспечению информационной безопасности позволяет оценить степень достижения поставленных целей, оценить соответствие принципам и рекомендациям, учитывать уровень сотрудничества с другими международными организациями, оценить вовлечение государств и стейкхолдеров, проанализировать результаты программ и проектов, а также оценить эффективность механизмов мониторинга и отчетности.

ЗАКЛЮЧЕНИЕ

В рамках данной работы мы исследовали роль Организации Объединенных Наций (ООН) в обеспечении международной информационной безопасности. Наш анализ позволил выявить ключевые аспекты и деятельность ООН в этой области, а также оценить эффективность ее подхода. В заключении хотелось бы подвести итоги и сделать основные выводы на основе полученных результатов. Важно содействовать активному участию государств и стейкхолдеров в разработке и реализации мер по обеспечению международной информационной безопасности.

Несмотря на значимость роли ООН в обеспечении международной информационной безопасности, существуют некоторые вызовы и проблемы, которые нужно учитывать. Одним из таких вызовов является быстрое развитие технологий, которое требует постоянного обновления и адаптации политик и подходов в области информационной безопасности. Кроме того, наблюдается рост киберугроз и киберпреступности, которые представляют серьезные вызовы для ООН и ее усилий в обеспечении информационной безопасности.

Сотрудничество с другими международными организациями также играет важную роль в эффективности подхода ООН. Международный союз телекоммуникаций (МСТ) и Международный союз электросвязи (ITU) являются примерами организаций, с которыми ООН взаимодействует и координирует свои усилия. Это сотрудничество способствует разработке общих стандартов и подходов к информационной безопасности.

Однако для эффективной работы ООН по обеспечению информационной безопасности необходимо учитывать вовлечение государств и стейкхолдеров. Оценка эффективности подхода ООН требует учета степени активного участия государств и других заинтересованных сторон в процессе разработки политики и реализации стратегий в области информационной безопасности.

Для преодоления данных вызовов и повышения эффективности подхода ООН к обеспечению информационной безопасности рекомендуется следующее:

- Укрепление сотрудничества с государствами и другими международными организациями: ООН должна продолжать развивать и укреплять свои партнерские отношения с другими организациями, такими как Международный союз телекоммуникаций и Международный союз электросвязи, для разработки общих стандартов и подходов к информационной безопасности;
- Продвижение и соблюдение международных норм и стандартов: ООН должна продолжать активно поощрять государства к соблюдению рекомендаций и принципов, предложенных организацией, таких как "Таллинская руководящая принципы в области национальной политики в киберпространстве" и "Киберстабильность";
- Усиление информационного обмена и обучения. ООН должна активно поддерживать инициативы, направленные на обмен информацией, передачу опыта и обучение в области информационной безопасности. Это позволит повысить осведомленность и подготовленность государств и стейкхолдеров к реагированию на киберугрозы.
- Повышение осведомленности и общественного участия: ООН должна активно работать над повышением осведомленности об информационной безопасности среди государств, организаций и общественности. Это может быть достигнуто путем проведения информационных кампаний, образовательных программ и создания платформ для обмена мнениями и передачи знаний о кибербезопасности;
- Содействие развитию технических возможностей: ООН должна поддерживать и поощрять развитие технических возможностей в области информационной безопасности. Это включает разработку инновационных технологий, инфраструктуры и инструментов, способствующих защите информации и противодействию киберугрозам.

В целом, ООН является важным международным актором в обеспечении международной информационной безопасности. Однако, для эффективной борьбы с вызовами и проблемами, связанными с информационной безопасностью, необходимо постоянное развитие и улучшение подходов, а также активное сотрудничество с государствами, международными организациями и другими заинтересованными сторонами. Только через совместные усилия и координацию действий можно достичь стабильности и надежности в международном киберпространстве.