ОТВЕТСТВЕННОСТЬ ГОСУДАРСТВА ЗА КИБЕРИНЦИДЕНТЫ И СТАНДАРТ «ДОЛЖНОЙ ОСМОТРИТЕЛЬНОСТИ» (DUE DILIGENCE)

Жоллыбаева Фатима Бахадыровна,
Магистрант факультета «Международное право»
Университета мировой экономики и дипломатии
ORCID: 0009-0006-3555-4865
e-mail: jollibaevafatima@gmail.com

Аннотация: *Данная работа посвящена проблеме международно-правовой ответственности государств за киберинциденты и роли принципа должной осмотрительности (due diligence) в контексте регулирования киберпространства. Актуальность темы обусловлена ростом числа и масштабов трансграничных кибератак, в том числе, совершаемых негосударственными субъектами с территории суверенных государств. В традиционном международном праве ответственность государства наступает за деяния, которые ему могут быть присвоены (attribution). Однако техническая сложность и проблема атрибуции кибератак существенно затрудняют применение классических норм. Анализируется содержание стандарта due diligence применительно к киберпространству, которое формируется на основе прецедентного права Международного Суда ООН (например, дело о проливе Корфу) и доктринальных разработок (например, Таллиннское руководство 2.0). Принцип должной осмотрительности рассматривается не как абсолютное обязательство предотвращения (duty of prevention), а как обязательство поведения (obligation of conduct), требующее от государства принятия разумных, адекватных и практически осуществимых мер для недопущения использования его киберинфраструктуры для действий, нарушающих права*

других государств, особенно в случаях, когда государство знало или должно было знать о такой активности. Работа выявляет существующие пробелы и неоднозначность толкования принципа due diligence в киберпространстве, подчеркивая необходимость достижения международного консенсуса для обеспечения стабильности и безопасности в сфере информационно-коммуникационных технологий (ИКТ).

Ключевые слова: *международно-правовая ответственность, киберинциденты (кибератаки), должная осмотрительность (due diligence), атрибуция (присвоение деяния государству), киберпространство, обязательство поведения (obligation of conduct), трансграничный вред, негосударственные субъекты, международное право (МП), таллиннское руководство (Tallinn Manual).*

Введение

Современное международное право сталкивается с беспрецедентными вызовами, порожденными стремительным развитием информационно-коммуникационных технологий. В условиях, когда киберинциденты приобрели трансграничный и геополитический характер, став инструментом государственного соперничества и нанеся значительный ущерб критической инфраструктуре (КИИ) по всему миру, вопрос о международно-правовой ответственности государств за вредоносную деятельность в киберпространстве приобрел критическую актуальность. Традиционный правовой механизм привлечения государства к ответственности за международно-противоправное деяние требует сложного процесса атрибуции – доказательства того, что кибероперация была совершена самим государством или под его эффективным контролем. Однако техническая природа кибератак, характеризующаяся высокой анонимностью, сложностью трассировки и возможностью использования прокси-серверов,

зачастую делает прямую атрибуцию практически невыполнимой. Эта правовая лакуна препятствует установлению порядка и стабильности в киберпространстве. В этом контексте стандарт «должной осмотрительности» (due diligence) выступает в качестве одного из наиболее перспективных правовых механизмов, позволяющих преодолеть трудности атрибуции, поскольку он смещает акцент с прямого участия государства в атаке на его обязанность по предотвращению вредоносной активности, исходящей с его территории.[1]

Таким образом, целью настоящего исследования является научное обоснование содержания и границ применимости стандарта должной осмотрительности как нормы международного обычного права и ключевого элемента ответственности государства за киберинциденты. Для достижения поставленной цели необходимо решить ряд задач: проанализировать прецедентное происхождение due diligence в международном праве (например, в деле о проливе Корфу), изучить и систематизировать критерии и разумные меры, составляющие содержание due diligence в контексте киберпространства, а также оценить ключевые проблемы его практического применения, такие как определение порога вреда и степени осведомленности государства.

Анализ литературы, посвященной данной проблематике, показывает, что концепция due diligence прочно укоренена в международном праве, что подтверждается статьями Комиссии международного права (КМП) об ответственности государств и решениями Международного Суда ООН (МС ООН). В контексте киберправа основным доктринальным источником является Таллиннское руководство 2.0 (Tallinn Manual on the International Law

[1] Кашкин, С. Ю., Четвериков, А. О. Международное публичное право. Учебник. М.: Проспект, 2022. (Раздел об ответственности государств).

Applicable to Cyber Operations), которое детально формулирует Правила 6–8, касающиеся обязанности государства проявлять должную осмотрительность. Обзор официальных позиций государств, высказанных в рамках Групп правительственных экспертов (ГПЭ) и Рабочей группы открытого состава (РГОС) ООН, выявляет растущий, хотя и не единогласный, консенсус относительно применимости due diligence к кибероперациям. При этом в научных публикациях отечественных и зарубежных авторов сохраняется активная дискуссия относительно юридической природы этой обязанности – является ли она обязательством поведения (obligation of conduct), требующим лишь принятия усилий, или обязательством результата (obligation of result), гарантирующим полное предотвращение вреда, – что требует дополнительного исследования.[2]

Я считаю, что актуальность и научная новизна темы определяются необходимостью выработки четких правовых критериев, которые позволили бы обеспечить баланс между суверенитетом государств и их ответственностью за действия в цифровой среде. Данное исследование, используя формально-юридический и сравнительно-правовой методы, стремится не только систематизировать существующие подходы к стандарту due diligence, но и предложить практические рекомендации по его конкретизации, тем самым внося вклад в формирование более устойчивого и предсказуемого правового режима в киберпространстве. Следующие разделы статьи будут посвящены анализу методов, результатов и обсуждению практических трудностей применения этого ключевого принципа.

Методы

[2] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Edited by Schmitt, M.N., and Vihul, L. Cambridge University Press, 2017. (Таллиннское руководство 2.0 по международному праву, применимому к кибероперациям).

Для достижения поставленной цели и решения обозначенных в начале работы задач исследование базировалось на комплексе общенаучных и частнонаучных методов. Прежде всего, был применен формально-юридический метод, который позволил провести детальный анализ и толкование международно-правовых документов, включая Проект статей об ответственности государств за международно-противоправные деяния Комиссии международного права (КМП), а также основополагающих доктринальных разработок, таких как Таллиннское руководство 2.0. Этот метод был решающим для определения юридической природы стандарта due diligence и его соотношения с традиционными нормами ответственности. В целях выявления общих принципиальных элементов стандарта и его специфики применительно к уникальной среде информационное пространство был использован сравнительно-правовой метод. Он позволил сопоставить применение due diligence в киберправе с его историческим прецедентным использованием в других отраслях международного права – в частности, в международном экологическом праве и в праве нейтралитета, основываясь на решениях Международного Суда ООН (например, дело о проливе Корфу).[3] Наконец, системный и функциональный анализ обеспечил понимание должной осмотрительности не как изолированной нормы, а как функционального элемента в общем механизме привлечения государства к ответственности, позволяющего эффективно обойти критические сложности атрибуции кибероперaций.

Результаты исследования.

В результате проведенного исследования и комплексного анализа международно-правовых источников и доктринальных разработок были получены основные выводы, касающиеся содержания и правовой природы

[3] International Court of Justice, Corfu Channel Case (United Kingdom v. Albania), 1949. (Международный Суд ООН, Дело о проливе Корфу).

стандарта **должной осмотрительности** (due diligence) в контексте международной ответственности государства за киберинциденты.

Стандарт «должной осмотрительности» (due diligence) — это правовое обязательство государства принимать разумные и адекватные меры для предотвращения использования своей территории в целях кибератак против других государств и для защиты собственной критической инфраструктуры, он не измеряется процентами и числами, а оценивается через призму международного и национального права. Тем не менее, масштабы киберинцидентов, по которым доступны официальные или полу-официальные статистические данные государственных органов Республики Узбекистан, напрямую влияют на объем усилий, которые государство должно предпринимать в рамках этого стандарта.

В Республике Узбекистан наблюдается значительный рост киберпреступности и активности кибератак:

- Динамика киберпреступлений: За последние пять лет (период, охватывающий приблизительно с 2019 по 2024 годы) число киберпреступлений в Узбекистане увеличилось примерно в 68 раз. Этот резкий рост демонстрирует нарастающую угрозу, требующую усиления мер со стороны государства.
- Финансовый ущерб: За период с 2021 по 2024 годы в результате киберпреступлений у граждан были похищены средства на сумму, превышающую 1,9 трлн сумов.
- Рост по годам: Только в 2024 году количество киберпреступлений возросло в 9,1 раза по сравнению с 2023 годом, а число обращений физических и юридических лиц о правонарушениях в киберпространстве увеличилось в 34 раза.
- Доминирующие угрозы: По данным МВД, 98% киберпреступлений составляют преступления, связанные с банковскими картами. Основные

схемы мошенничества включают получение SMS-кода для управления банковскими картами и мобильными приложениями (16% случаев), мошенничество на онлайн-торговых платформах (11%), а также оформление онлайн-кредитов на имя граждан (4%).

- Масштаб кибератак: За 2024 год в Узбекистане было зафиксировано более 12 млн попыток кибератак.

Угрозы для госсектора: За первый квартал 2024 года Центром кибербезопасности

Республики Узбекистан было выявлено и устранено 70 уязвимостей на государственных веб-ресурсах, а также опубликована статистика об инцидентах киберпреступности на 45 сайтах государственных органов. По секторам наибольшая часть киберугроз приходится на ИКТ (51,40%), государственный (24,20%) и финансовый (13,60%) секторы.

Глобальный контекст: В Глобальном индексе кибербезопасности (GCI) Узбекистан демонстрирует прогресс, войдя в категорию "T2 Advancing" (продвижение). Ранее, в 2021 году, индекс составлял 71,11, что подчеркивает заметный рост усилий в этой сфере, несмотря на сохраняющееся отставание по ряду показателей.

Эти данные отражают, что хотя юридическая ответственность государства является вопросом права, статистический рост числа и ущерба от инцидентов создает высокую потребность в последовательном и эффективном применении стандарта «должной осмотрительности» (due diligence) через реализацию национальных программ, совершенствование законодательства (например, Закона «О кибербезопасности» 2022 года) и усиление защиты критической информационной инфраструктуры для обеспечения безопасности граждан и стабильности государства.

Правовая природа Due Diligence

Прежде всего, было установлено, что стандарт должной осмотрительности является общепризнанным принципом международного обычного права, применимым в киберпространстве. Он квалифицируется как обязательство поведения (obligation of conduct), а не гарантированное обязательство результата (obligation of result). Этот ключевой вывод означает, что государство не несет абсолютной ответственности за любой киберинцидент, исходящий с его территории. Ответственность наступает исключительно за бездействие – то есть за непринятие разумных, адекватных и практически осуществимых мер по предотвращению или пресечению вредоносной активности, при условии, что государство знало или должно было знать о такой угрозе. Таким образом, due diligence является превентивной нормой, которая фокусируется на безответственность государства, а не на прямом участии в атаке.

Были четко определены пороговые условия, при которых возникает обязанность государства проявить должную осмотрительность в киберсфере:

1. Наличие Осведомленности (Knowledge): Государство должно было знать или должно было знать (knew or ought to have known) о готовящейся или совершающейся вредоносной активности. При этом, в отличие от физического мира, где знание часто является фактическим (например, нахождение военного лагеря), в киберпространстве преобладает критерий «должно было знать», основанный на разумных ожиданиях от функционирования служб кибербезопасности.[4]
2. Угроза Значительного Трансграничного Вреда (Threshold of Significant Harm): Обязанность due diligence запускается только в ответ на угрозу или реализацию существенного вреда другому государству. Это

[4] Articles on Responsibility of States for Internationally Wrongful Acts, 2001. (Статьи об ответственности государств за международно-противоправные деяния, принятые Комиссией международного права ООН).

отделяет международно-противоправное деяние от обычного киберкриминала.

Анализ результатов исследований.

Интерпретация полученных результатов выявляет ряд критических проблем и открытых вопросов, связанных с практическим применением стандарта должной осмотрительности (due diligence) в киберпространстве. Хотя установление due diligence как обязательства поведения (obligation of conduct) является фундаментальным, этот вывод немедленно порождает ключевую обсуждению о критериях его нарушения.

Как было показано в разделе «Результаты», должная осмотрительность функционирует как механизм, который обходит проблему сложной атрибуции (присвоения деяния государству). В то время как классическая ответственность требует доказательств эффективного контроля государ ства над субъектом, совершившим кибератаку, due diligence фокусируется на бездействии самого государства, то есть на его неспособности предотвратить известный или предсказуемый вред. Это сопоставление критически важно: принцип due diligence позволяет обеспечить стабильность в киберпространстве, даже когда последовательность операций доказательств вины обрывается на частном хакере или прокси-сервере. Это подтверждается доктриной Таллиннского руководства, которая прямо указывает, что отсутствие атрибуции не освобождает государство от обязанности проявлять должную осмотрительность.

Наиболее спорным аспектом, требующим глубокой интерпретации, остается критерий «должно было знать» (ought to have known). Сопоставление с прецедентами МС ООН (например, дело о геноциде и дело о проливе Корфу) показывает, что для установления ответственности необходимо доказать, что государство располагало фактическими или конструктивными знаниями об угрозе. В динамичной среде киберпространства это крайне сложно:

невозможно требовать от государства абсолютной осведомленности обо всех вредоносных действиях на своей территории. Интерпретировать этот критерий необходимо через призму технической разумности: государство должно было знать, если оно пренебрегло минимальными разумными шагами, такими как мониторинг критической инфраструктуры, анализ данных, предоставляемых международными партнерами, или отсутствие адекватного функционирования CSIRT/CERT-команд.[5]

Кроме того, требуется дальнейшее обсуждение порога значительного вреда. Доктринальные источники и некоторые государства-члены ООН соглашаются, что для активации due diligence необходим вред, существенный по своим последствиям (например, срыв работы больниц, финансового сектора или избирательных систем), даже если он не достигает порога применения силы. Этот подход, основанный на функциональном критерии вреда, позволяет международному праву адекватно реагировать на современные киберугрозы, не ограничиваясь исключительно военным контекстом.

Выводы и Рекомендации.

В заключение проведенного исследования следует однозначно констатировать, что стандарт должной осмотрительности (due diligence) подтверждает свою роль как основополагающего, обязательного и жизнеспособного принципа международного обычного права, применимого к поведению государств в киберпространстве. Главным выводом является то, что due diligence является обязательством поведения (obligation of conduct), и его применение является ключевым механизмом для обеспечения стабильности, поскольку он предоставляет легитимную правовую основу для привлечения государств к ответственности за невыполнение своих

[5] Тимофеев, Л. В. Международное право и киберпространство: проблемы ответственности государств // Московский журнал международного права. № 4, 2020. С. 15–28.

превентивных обязанностей, даже в условиях технической невозможности прямой атрибуции кибератаки. **** Успешная реализация этого принципа зависит от установления справедливого баланса между национальным суверенитетом и международной ответственностью.

Основные выводы:

1. Природа обязанности: Ответственность государства наступает за небрежное бездействие (непринятие разумных мер), а не за сам факт совершения атаки с его территории.
2. Условия активации: Обязанность due diligence активируется при наличии конструктивной осведомленности (государство «должно было знать») и угрозе значительного трансграничного вреда.
3. Дифференциация: Содержание «разумных мер» должно быть гибким и пропорциональным с учетом технологического потенциала и ресурсов конкретного государства.

Несмотря на доктринальный консенсус, для повышения эффективности и обеспечения правовой определенности в этой сфере требуется преодоление трех ключевых правовых пробелов. В этой связи, международному сообществу (например, в рамках ООН или региональных организаций) рекомендуется предпринять следующие меры:

1. Унификация критериев «Осведомленности»: Необходимо разработать объективные индикаторы и процедурные стандарты для определения того, когда государство, исходя из разумных ожиданий и доступных технологий, должно было знать о вредоносной активности, исходящей с его территории. Это снизит субъективность оценки.
2. Конкретизация Порога Вреда: Необходимо разработать руководство, которое четко определит, какой уровень нефизического ущерба (например, экономический или политический) считается «значительным» для запуска международно-правовой ответственности.

3. Создание Списка Типовых Мер: Следует разработать и принять международное руководство по минимальным разумным мерам (minimum reasonable steps), дифференцированное по уровню развития государств. Включение в него таких мер, как обязательное создание и финансирование CSIRT/CERT-команд, и стандартов международного обмена информацией, повысит прозрачность и предсказуемость поведения в киберпространстве.

Реализация данных рекомендаций позволит due diligence стать не просто теоретическим принципом, а эффективным, практически применимым инструментом поддержания стабильности и безопасности в сфере информационно-коммуникационных технологий.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Закон Республики Узбекистан от 15.04.2022 г. N ЗРУ-764 "О кибербезопасности" (Принят Законодательной палатой 25.02.2022 г., одобрен Сенатом 17.03.2022 г.)

2. Тимофеев, Л. В. Международное право и киберпространство: проблемы ответственности государств // Московский журнал международного права. № 4, 2020. С. 15–28.

3. Федоров, В. И. Принцип должной осмотрительности в международном праве: генезис и перспективы применения к киберконфликтам. М.: Норма, 2021.

4. Кашкин, С. Ю., Четвериков, А. О. Международное публичное право. Учебник. М.: Проспект, 2022. (Раздел об ответственности государств).

5. Articles on Responsibility of States for Internationally Wrongful Acts, 2001. (Статьи об ответственности государств за международно-противоправные деяния, принятые Комиссией международного права ООН).

6. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Edited by Schmitt, M.N., and Vihul, L. Cambridge University Press, 2017. (Таллиннское руководство 2.0 по международному праву, применимому к кибероперациям).

7. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (Доклад Группы правительственных экспертов ООН). Документы ООН (например, A/73/305, A/65/201).