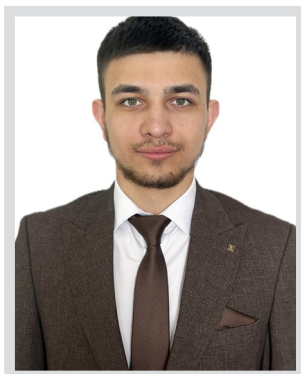


УДК. 341.1/8

DOI: 10.24412/1998-5533-2026-1-143-149

**Кибербезопасность и информационная безопасность:
правовые проблемы терминологической дифференциации
в международном и внутригосударственном праве**



Гайсин Реналь Радикович

Аспирант кафедры международного права
Казанского (Приволжского) федерального университета

В условиях перманентно усиливающихся информационных угроз возрастает необходимость понимания сущности кибербезопасности и информационной безопасности. В международных актах, законодательстве ряда государств и научной доктрине накопилось множество проблем терминологического характера, связанных с трактовкой понятий «кибербезопасность», «информационная безопасность» и других схожих понятий.

Цель научного исследования заключается в выявлении и анализе основных терминов и концепций понимания кибербезопасности и информационной безопасности.

Результаты статьи могут быть полезны в исследовательских, образовательных и практических целях. Ценность работы заключается в расширении знаний исследователей и практиков о природе кибербезопасности и информационной безопасности.

В рамках исследования юридической природы рассматриваемых терминов проводится разграничение и обосновывается позиция относительно их применения. Подтверждается существование двух противоречивых концепций понимания кибербезопасности и информационной безопасности.

Ключевые слова: кибербезопасность, информационная безопасность, киберпространство, цифровая безопасность, безопасность информации, безопасности в сфере использования информационно-коммуникационных технологий, киберконфликт, кибероперации

Для цитирования: Гайсин Р.Р. Кибербезопасность и информационная безопасность: правовые проблемы терминологической дифференциации в международном и внутригосударственном праве // Вестник экономики, права и социологии. 2026. № 1. С. 143–149. DOI: 10.24412/1998-5533-2026-1-143-149.

«...В переполненной матрице, монохромном псевдопространстве, где, как редкие звезды во тьме, светились плотные сгустки данных, мерцали галактики корпораций и отсвечивали холодным блеском спирали военных систем...». Таково описание киберпространства, которое У. Гибсон приводит в своем научно-фантастическом рассказе «Сожжение Хром» [1]. Идея о существовании некоего нового пространства с большими возможностями издавна увлекала умы, но своей кульминации она достигла

в конце XX в., в эру компьютеров и программистов. Гибсон называет своего героя – программиста-хакера по имени Бобби – «ковбоем, оседлавшим компьютер». Сравнение киберпространства с Диким Западом неслучайно. Киберпространство – это действительно современный Дикий Запад, где правота определяется силой, где ответственность может не догнать виновного, а угроза таится за каждой каменной стеной. В безопасности находится лишь тот, кто вооружен и может первым ответить на угрозу.

И не случайно первый рассказ о киберпространстве иллюстрирует нам взлом информационной системы, то есть описывает угрозу кибербезопасности.

Сегодня вопросы обеспечения кибербезопасности имеют большую актуальность, и центральный элемент проблемы, представляющий научный интерес, – это разграничение понятий «кибербезопасность», «информационная безопасность» и других смежных терминов. Ведь наиболее острые дискуссии на международных площадках в сфере международной информационной безопасности разворачиваются вокруг трактовки этих терминов и связанных с ними смысловых аспектов. Очевидно, *ab initio* большинство терминов формируется исходя из признаков, свойств и других характеристик изучаемых правовых явлений. Расхождение в них разумно предполагает отсутствие единства в других, не менее важных вопросах.

Являясь свидетелями эпохи турбулентности международных отношений, нельзя исключать и политический аспект. *Cui prodest?* – звучит латинское выражение, означающее, что в любом вопросе есть выгода и есть сторона, которая хочет ее получить. Существует мнение, что на протяжении ряда лет США и другие западные страны выступают за использование термина «кибербезопасность» вместо понятий «информационная безопасность» и «международная информационная безопасность», чтобы сохранить и приумножить возможности для внешнего вмешательства в системы информационной безопасности неугодных им суверенных государств [2]. В качестве аргументов они используют нарративы защиты прав человека и стремление противодействовать цифровому авторитаризму государств [3].

Закрепление определения – это очерчивание границ регулирования. Почему во многих определениях кибербезопасности акцентируется внимание только на техническую часть вопроса, не затрагивая при этом информационные и психологические аспекты? Что понимается под обороной киберпространства? Это противодействие кибератакам или проведение наступательных киберопераций, направленных против государств? Эти и другие вопросы сегодня стоят перед исследователями многих стран, и мы попытаемся на них ответить.

Сегодня вокруг концепции кибербезопасности ведется множество обсуждений, а сам термин трудно поддается определению и является предметом политических споров. К примеру, Организация экономического сотрудничества и развития (ОЭСР) использует термин «цифровая безопасность» [4], Шанхайская организация сотрудничества (ШОС) использует термин «информационная безопасность» [5], Европейский союз (ЕС) использует термин «кибербезопасность» и «безопасность информации» [6], Организация Объединенных Наций (ООН) в некоторых документах использует термин

«безопасность в сфере использования информационно-коммуникационных технологий» [7]. Как отмечает в своем исследовании Т. Насименто Хайм, эти различия в понимании и интерпретациях значения и содержания кибербезопасности, с одной стороны, отражают политический и культурный выбор национальных государств, а с другой – затрудняют нормативное регулирование киберпространства [8].

Более того, концепция кибербезопасности постоянно эволюционирует: возникшая как часть технической проблемы или проблемы управления рисками в течение пары лет, она превратилась в вопрос национальной и международной безопасности [9, p. 73]. Соответственно, терминология, используемая для обсуждения аспектов безопасности технических устройств и информации, значительно изменилась в последние годы. Так, если в начале века термины, которые регулярно использовались в этом контексте, были «компьютерная безопасность», «сетевая безопасность», «Интернет-безопасность», «безопасность информации», то сейчас к ним добавились «кибербезопасность», «информационная безопасность» и «цифровая безопасность».

Научный мир признает, что отсутствие согласованного значения термина «кибербезопасность» является существенной проблемой. Этому посвящены исследования таких зарубежных исследователей, как К. Байлон [10], Д. Крейген [11], Д. Шатц [12], М.Д. Кавелти [13] и др. Упомянутая проблема усугубляется проблемой различия других понятий в области кибербезопасности. Определения таких терминов, как «киберконфликт», «кибервойна», «кибератака» и т.д., используемые США, Великобританией, Россией и Китаем, не совпадают – даже если официальные определения существуют в каждом соответствующем языке. К. Джайлс и В. Хагстад утверждают, что прямые переводы конкретных терминов с русского и китайского языка, которые напоминают англоязычные термины и наоборот, могут еще больше усложнить ситуацию, создавая обманчивое впечатление взаимопонимания, хотя на самом деле они относятся к совершенно разным концепциям [14].

В связи с этим разумно будет обратиться к этимологии. Деконструкция термина «кибербезопасность» позволит расположить обсуждение в рамках обеих областей – «кибер» и «безопасности» – и раскрыть некоторые особенности их происхождения с точки зрения лингвистики и герменевтики.

Как известно, приставка «кибер» («*cyber*») произошла от термина «кибернетика», который относится к области «теории управления и связи в машинах и живых организмах» [15]. Термин «кибернетика» берет начало с древнегреческого слова *κυβερνάω*, что означает «рулить», «управлять» [16]. Теория об изучении взаимодействия человека и техники, где непрерывен информационный поток между управ-

ляющим и управляемым, легла в основу феномена кибернетического пространства (киберпространство – «*cyberspace*») Впервые термин «киберпространство» был использован в 1982 г. У. Гибсоном в рассказе «Сожжение Хром». В дальнейшем это слово использовалось в других его произведениях, что и стало точкой отсчёта, после которой идеи киберпространства получили широкое распространение и породили множество терминов с приставкой «кибер-».

Что касается термина «безопасность», в зарубежной и отечественной научной литературе не существует общепринятой концепции, и этот термин, как отмечается, трудно определить в общем смысле. К примеру, Оксфордский словарь английского языка содержит около двадцати значений этого слова [17]. Толковый словарь В. Даля определяет безопасность как «отсутствие опасности, сохранность, надёжность» [18]. В Толковом словаре русского языка С.И. Ожегова безопасность понимается как «состояние, при котором не угрожает опасность» [19]. Таким образом, в указанных словарях понятие безопасность раскрывается по-разному, однако можно выделить общий смысловой аспект – отсутствие опасности или угрозы.

Сегодня в научной литературе и законодательстве западных стран преобладает техническая точка зрения на природу кибербезопасности. Так, Р.А. Кеммерер утверждает, что кибербезопасность «в основном состоит из защитных методов, используемых для обнаружения и пресечения потенциальных злоумышленников» [20]. Схожее определение приводит Дж.А. Льюис в своем исследовании, указывая, что кибербезопасность «подразумевает защиту компьютерных сетей и хранящихся в них информации от проникновения и злонамеренного повреждения или нарушения» [21]. Э. Аморосо видит кибербезопасность как «снижение риска вредоносных атак на программное обеспечение, компьютеры и сети» [22]. В качестве примера законодательного закрепления можно привести Национальную стратегию кибербезопасности Канады, где кибербезопасность обозначается как «защита цифровой информации, а также целостность инфраструктуры размещения и передачи цифровой информации» [23].

Если обратиться к международным стандартам, то можно увидеть, что в соответствии с ISO/IEC 27032:2023 [24], кибербезопасность определяется как «защита людей, общества, организаций и наций от киберрисков». Ранее действовавший стандарт ISO/IEC 27032:2012 [25], обозначал кибербезопасность как «сохранение конфиденциальности, целостности и доступности информации в киберпространстве». Данное определение было сформировано исходя из понятия «безопасность информации», которая содержит триаду свойств информации: конфиденциальность, целостность и доступность (так называемое определение *CIA*).

Стоит добавить уточнение, что в англоязычных странах термины «безопасность информации» и «информационная безопасность», которые в российском понимании имеют разные значения, лингвистически не различаются, поскольку перевод обоих слов на английский язык одинаковый (*information security*). В стандарте, как уже отмечено, подразумевается именно «безопасность информации», то есть такое состояние, при котором информация находится в безопасности.

По мнению исследователей Б. Лундгрена и Н. Мёллера [26, р. 422], понятие «безопасность информации» имеет ряд недостатков:

1. Оно является одновременно слишком широким и слишком узким;

2. Его предполагаемые необходимые свойства не во всех случаях являются необходимыми. Более того, в зависимости от ситуации, одному из свойств может отдаваться приоритет по отношению к другим, что ставит под сомнение их необходимость.

Хотя некоторые из вышеуказанных определений включают ссылки на нетехнические действия и человеческие взаимодействия, такой подход отличается от видения, которого придерживаются Россия, Китай и страны ШОС. Согласно Приложению 1 к Соглашению между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, под информационной безопасностью понимается «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве».

В научной литературе этот подход получили название «восточного видения» [27, р. 552], данная концепция информационной безопасности имеет более широкий охват, так как помимо информации и технических средств как объектов безопасности включает ряд других объектов, таких как личность, общество и государство. Соответственно, угрозы, которые могут оказать негативное воздействие, имеют не только технический характер, но и включают информационные и психологические способы воздействия на сознание.

Помимо отражения подходов соответствующих государств к природе информационной безопасности, это различие в подходах между двумя группами государств наглядно иллюстрирует также различие в концепциях регулирования интернета, которое препятствует международному взаимопониманию: западный взгляд на открытое, свободное и глобальное пространство, эффективно управляемое широким кругом заинтересованных сторон, в том числе неправительственными организациями, в отличие от восточного взгляда, поддерживаемого Россией, Китаем и рядом других стран, где именно государ-

ство несет ответственность за внутреннее информационное пространство.

Термин «кибербезопасность» не существует в российском законодательстве, а представленный в 2014 г. проект «Концепция стратегии кибербезопасности Российской Федерации» [28] не нашел поддержки в связи с несоответствием терминологии, указанной в Доктрине информационной безопасности Российской Федерации [29]. Однако в законодательстве ряда стран-партнеров, например Республики Беларусь [31] и Республики Казахстан [32], термины «информационная безопасность» и «кибербезопасность» (последний с существенно иной интерпретацией) используются как синонимы.

Следует сказать, что вопрос о природе кибербезопасности корнями уходит к проблеме применимости международного права к киберпространству. Киберугрозы отличаются от традиционных проблем безопасности прежде всего в том, что касается принадлежности и юрисдикции, поскольку кибератака может быть инициирована из любой точки планеты [33]. Следовательно, важные принципы права, такие как самооборона и вооруженное нападение, основанные на территориальных представлениях, не применимы автоматически.

Западные страны выступают за возможность применения международного права в нынешнем виде, в частности международного гуманитарного права и международного права прав человека, к регулированию военных действий в киберпространстве. С противоположной позицией выступают Россия и Китай, которые считают, что информационное пространство должно быть демилитаризованным. В то время как в рамках ООН следует принять согласованный международный правовой акт по обеспечению международной информационной безопасности.

Поэтому существуют определения кибербезопасности, лейтмотивом которых является концепция киберконфликта. Согласно данной концепции, если раньше основными аренами боевых действий были земля, море и воздух, то теперь война перешла в «четвертую плоскость» – киберпространство, что привело к значительному сдвигу в способах ведения войны. Эта идея весьма отчетливо отражена в документе варшавского саммита НАТО «Обязательство по киберобороне» [34].

Пример такого определения содержится в стратегии кибербезопасности Новой Зеландии [35], где кибербезопасность видится как «практика создания сетей, составляющих киберпространство, насколько возможно защищенных от вторжений, поддерживающих конфиденциальность, целостность и доступность информации, обнаружение происходящих вторжений и инцидентов, реагирование и восстановление после них». Национальный институт стандартов и технологий (*NIST*) определяет кибер-

безопасность как «способность защищать и оборонять киберпространство от кибератак» [36]. В законодательстве Великобритании, Франции, Польши и других стран не приводятся определения, но исходя из анализа стратегических документов, можно вывести схожие позиции относительно этого термина.

Может показаться, что на первый взгляд нынешнее понимание кибербезопасности этих стран основывается на обороне и защите. Однако при детальном рассмотрении оказывается, что аналогии с физическим миром не могут быть применены к киберпространству. Более того, слова «киберзащита» и «кибероборона» в американском понимании предполагают заблаговременное применение силы перед лицом неизбежного нападения. Так, согласно документу «Концептуальный план возможностей армии США для операций в киберпространстве (*CyberOps*) на 2016–2028 годы» [37], киберзащита предполагает в том числе «максимальное использование наступательных действий для противодействия киберугрозам». С учетом способности маскировать государственную принадлежность в киберпространстве и возможности предписывания действий негосударственных субъектов конкретному государству существует риск широкой трактовки норм международного права, в частности ст. 51 Устава ООН, которая дает право государству ответить на нападение любыми доступными средствами (право на самооборону) для оправдания проведения кибероперации против другого государства [38, с. 86].

Ярким примером этих противоречий служит Глобальный цифровой договор [39], принятый 22 сентября 2024 г. в рамках Саммита будущего ООН. Данный документ представляет собой универсальный инструмент мягкого права [40], который нацелен на то, чтобы привести к единству участников глобального цифрового взаимодействия и определить основные ориентиры на ближайшие годы. Однако сформулированные в договоре положения носят несбалансированный характер [41], поскольку уравнивают роль государств, неправительственных организаций и транснациональных корпораций, а также акцентируют значимость прав человека в западном видении и не учитывают принцип государственного суверенитета [42, с. 67]. Кроме того, документ предусматривает создание дополнительных обзорных механизмов с неясными мандатами [43].

Предложенная российской стороной поправка о невмешательстве ООН во внутренние дела других стран, основанная на п. 7 ст. 2 Устава ООН, была отклонена на заседании Генеральной Ассамблеи ООН всеобщим голосованием [44]. Против отклонения поправки, помимо России, выступили также Белоруссия, Никарагуа, Северная Корея, Сирия, Судан и Иран. Еще 15 стран воздержались от голосования, в то время как 143 государства поддержали предложение об отклонении.

Проблематика реформирования Совета Безопасности ООН, являющаяся основной идеей в Пакте будущего [45], представляется крайне важной для развивающихся стран, в связи с чем большинство из них приняли решение поддержать данный документ. Так как Глобальный цифровой договор был представлен как одно из приложений к Пакту будущего наряду с Декларацией о будущих поколениях [46], отказ от голосования в поддержку данного документа означал бы отказ от поддержки Пакта будущего – ключевого документа, направленного на вывод ООН из системного кризиса.

Таким образом, на основе обзора законодательства и научной литературы можно сделать вывод, что определения «кибербезопасности» и «информационной безопасности» сильно различаются, а дискуссия, разворачивающаяся вокруг них, по большей части политизирована и зависит от национальных особенностей. Это приводит к разнообразию концепций, касающихся сферы применения и значения терминологии. В этом контексте такие термины, как «компьютерная безопасность», «безопасность информации», «цифровая безопасность», «информационная безопасность» используются альтернативно, часто как синонимы «кибербезопасности» зарубежными учеными при описании точного содержания. Это усиливает преимущественно узкий, технический взгляд на природу информационной безопасности. Неясные определения, допускающие различное толкование, оставляют возможность для использования норм международного права в угоду политическим амбициям.

В то же время следует отметить, что по большому числу вопросов кибербезопасности мнение американских и других западных экспертов совпадает. Это позволяет говорить о том, что научное и экспертное сообщество западных государств выработало определённое представление о природе кибербезопасности и активно занимается его продвижением в рамках ООН, G7, G20 и других соответствующих многосторонних форумов. Россия и Китай также не изолированы в своих взглядах на информационную безопасность: существует большое количество других государств, которые разделяют их взгляды и их обеспокоенность по поводу цифрового суверенитета. Несомненно, что при отсутствии общности взглядов на природу и регулирование кибербезопасности любой потенциал для установления общепризнанной терминологии в этой области остается отдаленным.

Однако Дикий Запад по истечении времени все же перестал быть «диким», а некогда царившее правило «прав тот, кто сильнее» сменилось законами и порядком. Скорее всего, киберпространство ожидает такая же перспектива. Возможно, факт принятия первого в мире международного акта в области информационной безопасности – Конвенции ООН про-

тив киберпреступности [47], а также намечавшаяся перезагрузка отношений между США и Россией, позволит начать конструктивный диалог в рамках гармонизации западного и восточного взглядов на концепцию кибербезопасности и информационной безопасности.

Литература:

1. Gibson W. *Burning Chrome*. New York: Arbor House, 1986. 200 p.
2. Кузьмин А., Жуков Ю., Финогенов Д. Терминология в сфере международной информационной безопасности // *BIS Journal*. 2015. № 3(18). URL: https://archive.org/details/DTIC_ADA516590 (дата обращения: 02.02.2025)
3. Declaration for the Future for the Internet. URL: <https://www.state.gov/declaration-for-the-future-of-the-internet> (дата обращения: 28.02.2025).
4. Recommendation of the Council on Digital Security of Critical Activities. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456> (дата обращения: 02.03.2025).
5. Крутских А.В. *Международная информационная безопасность: Теория и практика: В 3 т. Т. 2: Сб. документов (на русском языке)*. М.: Издательство «Аспект Пресс», 2019. 784 с.
6. Гирис В.А. Понятие «кибербезопасность» в праве Европейского союза // *Юридическая наука*. 2022. № 7. С. 115–120.
7. Резолюция ГА ООН A/RES/76/19 от 6 декабря 2021 г. URL: <https://undocs.org/ru/A/RES/76/19> (дата обращения: 02.03.2025).
8. Nascimento Heim T. Global governance and regulation of cybersecurity: towards coherence or fragmentation? URL: https://www.academia.edu/103247252/Global_governance_and_regulation_of_cybersecurity_Towards_coherence_or_fragmentation (дата обращения: 01.03.2025).
9. Nissenbaum H. Where computer security meets national security? // *Ethics and Information Technology*. 2005. № 10. P. 61–73.
10. Baylon K. Challenges at the Intersection of Cyber Security and Space Security Country and International Institution Perspectives. URL: https://www.academia.edu/21723170/Challenges_at_the_Intersection_of_Cyber_Security_and_Space_Security_Country_and_International_Institution_Perspectives (дата обращения: 01.03.2025).

11. Craigen D., Diakun-Thibault N., Purse R. Defining Cybersecurity // *Technology Innovation Management Review*. 2014. Vol. 4. № 10. P. 13–21.
12. Schatz D., Bashroush R., Wall J. Towards a more representative definition of cyber security // *Journal of Digital Forensics, Security and Law*. 2017. Vol. 12. № 2. P. 53–74.
13. Cavelti M.D., Egloff F.J. The Politics of Cybersecurity: Balancing Different Roles of the State // *St Antony's International Review*. 2019. Vol. 15. № 1. P. 37–57.
14. Giles K., Hagestad W. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. URL: https://www.researchgate.net/publication/261300676_Divided_by_a_common_language_Cyber_definitions_in_Chinese_Russian_and_English (дата обращения: 28.02.2025).
15. Wiener N. *Cybernetics: Or Control and Communication in the Animal and the Machine*. Cambridge Massachusetts (MIT Pre Press), 1965. 231 p.
16. Дворецкий И.Х. Древнегреческо-русский словарь. М.: Государственное издательство иностранных и национальных словарей, 1958. Т. 1. 1043 с.
17. Oxford English Dictionary. URL: <https://www.oed.com/> (дата обращения: 02.03.2025).
18. Даль В.И. Толковый словарь живого великорусского языка. М.: Русский язык, 1989. 708 с.
19. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 72500 слов и 7500 фразеологических выражений. М.: Азъ, 1994. 907 с.
20. Kemmerer R.A. Cybersecurity // *Proceedings of the 25th IEEE International Conference on Software Engineering*. 2003. P. 705–715.
21. Lewis J.A. Cybersecurity and Critical Infrastructure Protection. URL: https://www.researchgate.net/publication/266496960_Cybersecurity_and_Critical_Infrastructure_Protection (дата обращения: 05.03.2025).
22. Amoroso E. *Cyber Security*. New Jersey: Silicon Press, 2006. 200 p.
23. Canada's National Cyber Security Strategy. URL: <https://cctx.ca/wp-content/uploads/2025/02/2025-National-Cyber-Security-Strategy.pdf> (дата обращения: 05.03.2025).
24. ISO/IEC 27032 Information technology. Security techniques. Guidelines for cybersecurity. URL: <https://www.iso.org/standard/44375.html> (дата обращения: 02.03.2025).
25. ISO/IEC 27032:2023. Cybersecurity. Guidelines for Internet security. URL: <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27032:ed-2:v1:en> (дата обращения: 02.03.2025).
26. Lundgren B., Moller N. Defining Information Security // *Sci Eng Ethics*. 2019. № 25. P. 419–441.
27. Alcantara B.T. SCO and Cybersecurity: Eastern Security Vision for Cyberspace // *International Relations and Diplomacy*. 2018. Vol. 6. № 10. P. 549–555.
28. Концепция кибербезопасности разошлась с государственной стратегией. URL: <https://www.kommersant.ru/doc/2355154> (дата обращения: 04.03.2025).
29. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // *СЗ РФ*. 2016. № 50. Ст. 7074.
30. Мартиросян А.Ж. Международно-правовое регулирование обеспечения безопасности в сфере использования информационно-коммуникационных технологий: дис ... канд. юрид. наук. М., 2024. 202 с.
31. Указ Президента Республики Беларусь от 14.02.2023 № 40 «О кибербезопасности». URL: <https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g> (дата обращения: 05.03.2025).
32. Постановления Правительства Республики Казахстан от 30.06.2017. № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)». URL: <https://adilet.zan.kz/rus/docs/P1700000407/links#to> (дата обращения: 05.03.2025).
33. Pernice I. Global cybersecurity governance: A constitutionalist analysis // *Global Constitutionalism*. 2018. Vol. 7. Iss.1. P. 112–141.
34. Cyber Defence Pledge. URL: https://www.nato.int/cps/en/natohq/official_texts_133177.htm (дата обращения: 05.03.2025).
35. New Zealand's cyber security strategy. URL: https://sherloc.unodc.org/cld/ru/treaties/strategies/new_zealand/nzl0004s.html (дата обращения: 05.03.2025).
36. The National Institute of Standards and Technology Cybersecurity Framework (CSF) 2.0. URL: <https://www.nist.gov/cyberframework> (дата обращения: 05.03.2025).
37. Cyberspace Operations Concept Capability Plan 2016–2028. URL: https://archive.org/details/DTIC_ADA516590 (дата обращения: 04.03.2025).
38. Карасев П.А. Эволюция национальных подходов к ведению кибервойны // *Международная аналитика*. 2022 № 13(2). С. 79–94.
39. Глобальный цифровой договор. URL: <https://www.un.org/ru/summit-of-the-future/global-digital-compact> (дата обращения: 07.04.2025).
40. Глобальный цифровой договор ООН: упорядочение хаоса или следование интересам транснационального бизнеса? URL: <https://cgitc.ru/media/globalnyy-tsifrovoy-dogovor-oon-uporyadochenie-khaosa-ili-sledovanie-interesam-transnatsionalnogo-bi/> (дата обращения: 12.04.2025).
41. Что не так с Глобальным цифровым договором? URL: <https://russiancouncil.ru/analytics-and-comments/analytics/chto-ne-tak-s-globalnym-tsifrovym-dogovorom/> (дата обращения: 07.04.2025).
42. Зиновьева Е.С. *Международное управление Интернетом*. М.: 2025. 186 с.

43. Выступление заместителя Министра иностранных дел Российской Федерации С.В. Вершинина на «Саммите будущего», Нью-Йорк, 23 сентября 2024 года. URL: https://www.mid.ru/ru/foreign_policy/news/1970892/ (дата обращения: 12.04.2025).
44. Умнова-Конюхова И.А. Пакт ООН во имя будущего и взгляд России на новый международный правопорядок // Baikal Research Journal. 2024. Т. 15. № 4. С. 1381–1390.
45. Пакт во имя будущего. URL: <https://www.un.org/ru/summit-of-the-future/pact-for-the-future> (дата обращения: 12.04.2025).
46. Декларация о будущих поколениях. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-1-Annex-II> (дата обращения: 12.04.2025).
47. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243> (дата обращения: 05.03.2025).

Cybersecurity and Information Security: Legal Problems of Terminological Differentiation in International and Domestic Law

Gaisin R.R.
Kazan (Volga Region) Federal University

In the context of constantly increasing information threats, there is an increasing need to understand the essence of cybersecurity and information security. A number of terminological problems related to the interpretation of the concepts of «cybersecurity», «information security» and other similar concepts have accumulated in international acts, legislation of a number of States and scientific doctrine.

The purpose of the scientific research is to identify and analyze the basic concepts of understanding cybersecurity and information security.

The results of the article can be useful for research, educational and practical purposes. The value of the work lies in expanding the knowledge of researchers and practitioners about the nature of cybersecurity and information security.

As part of the study of the legal nature of the terms under consideration, a distinction is made and a position regarding their application is substantiated. The existence of two contradictory concepts of understanding cybersecurity and information security is confirmed.

Keywords: cybersecurity, information security, cyberspace, digital security, information security, security in the use of information and communication technologies, cyber conflict, cyber operations

