УДК 341.1 https://doi.org/10.33619/2414-2948/85/52

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МЕЖДУНАРОДНОМ ПРАВЕ

©Бердимуратова Г. М., *Ph.D., Каракалпакский государственный университет им. Бердаха, г. Нукус, Узбекистан, berdimuratovagulnaz91@gmail.com*

ISSUES ON ENSURING INFORMATION SECURITY IN INTERNATIONAL LAW

©Berdimuratova G., *Ph.D., Karakalpak State University named after Berdakh, Nukus, Uzbekistan, berdimuratovagulnaz91@gmail.com*

Аннотация. На международной арене проблема обеспечения международной информационной безопасности приобретает все более глубокое значение осуществляются программные меры в целях правового обеспечения информационной безопасности, предупреждения и борьбы с правонарушениями и преступлениями в сфере информационных технологий. В этой связи установление ответственности за распространение информации, представляющей угрозу правам и свободам личности, интересам общества и государства, охрана информационной безопасности в качестве объекта уголовно-правовой охраны, разработка комплекса мер по противодействию информационным преступлениям являются актуальными задачами. Представлен теоретический и практический анализ международноправовых аспектов информационной безопасности, рассматриваются этапы, и пробелы в этой сфере, вносится предложения по совершенствованию действующего законодательства.

Abstract. In the international arena, the problem of ensuring international information security is becoming increasingly important; program measures are being taken to legally ensure information security, prevent and combat offenses and crimes in the field of information technology. In this regard, the establishment of responsibility for the dissemination of information that poses a threat to the rights and freedoms of the individual, the interests of society and the state, the protection of information security as an object of criminal law protection, the development of a set of measures to combat information crimes are urgent tasks. This article provides a theoretical and practical analysis of the international legal aspects of information security, discusses the stages and gaps in this area, and makes suggestions for improving the current legislation.

Ключевые слова: информационная безопасность, информационная сфера деятельности, информационные технологий, охрана данных, кибербезопасность, интернет.

Keywords: information security, information field of activity, information technologies, data protection, cybersecurity, internet.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования

Т. 8. №12. 2022
https://doi.org/10.33619/2414-2948/85

возникающих при этом общественных отношений.

В свою очередь, президент Ш. Мирзиеев справедливо указывает, что «...необходимо учесть и использовать значительные преимущества современных компьютерных технологий и особенно сети Интернет» (https://goo.su/WjwRIQ).

Стремительный рост информационных технологий в различных сферах человеческой деятельности, с одной стороны, позволил обеспечить высокие достижения и результаты, а с другой стороны, стал источником самых непредсказуемых и вредных последствий для человеческого общества. В результате можно говорить о появлении принципиально нового сегмента международного противоборства, затрагивающего как вопросы безопасности отдельных государств, так и общую систему международной безопасности на всех уровнях.

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

Существуют различия в подходах к определению понятия «информационная безопасность». В национальном законодательстве понятие «информационная безопасность» сводится к «состоянию защищенности интересов личности, общества и государства в информационной сфере» (https://lex.uz/docs/52709).

В зарубежных правовых актах (в частности, американских) информационная безопасность определяется не просто как состояние защищенности информационной среды, а как «способность сети или системы противостоять с нужным уровнем надежности авариям или злонамеренным действиям, которые могут нарушить доступность, целостность и конфиденциальность хранимой и передаваемой информации» (https://goo.su/yTq6Al).

В соответствии со ст. 3 «Закона о кибербезопасности Республики Узбекистан», кибербезопасность — это состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве (https://lex.uz/en/docs/5960609).

По определению Н. А. Нугманова, информационная безопасность — это состояние общества, при котором обеспечена надежная и всесторонняя защита личности, общества и государства в информационном пространстве от воздействия на них особого вида угроз, выступающих в форме организованных или стихийно возникающих информационных и коммуникационных потоков [1].

А. А. Стрельцов считает, что во многих определениях информационной безопасности делается акцент на состоянии внешней среды. Информационная безопасность, по существу, отражает не столько статическое состояние социума, сколько его динамику, то есть взаимодействия общественных и государственных структур по предотвращению угроз в информационной сфере. Исходя из этого информационная безопасность определяется, как состояние институтов государства и общества, при котором обеспечивается надежная защита национальных интересов страны и ее населения в информационной сфере [2].

В данном определении подчеркивается основная предпосылка защиты национальных интересов — необходимое состояние государственных институтов и гражданского общества. Именно на государство и общественные структуры возлагается обязанность обеспечения информационной безопасности.

Более конкретно данное понятие раскрывается А. В. Кисляковским, информационная безопасность — это право общества на получение достоверной информации, сохранение тайны и конфиденциальных сведений путем противодействия перехвату, прослушиванию передаваемых сообщений, проникновению в компьютерные сети; защита личности и общества от воздействия на них информационно-психологических угроз, диффамации и

Т. 8. №12. 2022
https://doi.org/10.33619/2414-2948/85

клеветы; борьба с преступностью в сфере информационных и телекоммуникационных систем для обеспечения организационной и личной безопасности [3].

Отметим, что в последние годы среди западных исследователей появляются представители сдержанного подхода, подчеркивающие значимость политико-идеологической составляющей угроз информационной безопасности. В частности, М. Данн-Кавелти, сотрудник Центра исследований безопасности в Швейцарии полагает, что проблема информационной безопасности несводима исключительно к инфраструктурной составляющей, к кибератакам или киберинцидентам [4].

Редакторы сборника «Международные отношения и безопасность в цифровую эпоху» используют термины «информационная война», но «кибер-терроризм» и «кибер-преступность», таким образом, признавая значимость политико-идеологического противостояния в межгосударственных отношениях и обеспечении безопасности в условиях информационной революции [5].

Д. Най также отмечает значимость информационного воздействия в обеспечении безопасности в конфликтах. Он полагает, что в современных конфликтах, военные силы и нерегулярные силы, комбатанты и гражданское население, физическое разрушение и информационное воздействие тесно переплетены. Более того, наличие камер в каждом мобильном телефоне и программы для редактирования фото на каждом компьютере, лишь усиливают информационную составляющую современного межгосударственного противостояния [6].

Таким образом, существующие определения информационной безопасности можно классифицировать на три группы. Во-первых, информационная безопасность как непосредственное состояние защищенности интересов, личности, общества и государства в информационной сфере. Во-вторых, информационная безопасность как состояние социально-политической среды, при котором обеспечивается защита личности, общества, государства. В-третьих, информационная безопасность как право, гарантия получения достоверной информации.

Международная информационная безопасность определяется ООН как «состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве» [7].

Представленные взгляды ученых на понятие и проблему информационной безопасности обнаруживают как наличие общих взглядов, так и специфику каждого их подходов. Однако, ясно одно: решение проблем информационной безопасности, возможно только за счет скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер.

Действующее международное право довольно неоднозначно регулирует многие вопросы информационной безопасности. Например, рассмотрим, насколько легальна в соответствии с международным правом, является информационная война, которая в последнее время все чаще и чаще применяется в вооруженных конфликтах.

По мнению А. В. Крутского, информационная безопасность, как самостоятельная категория, возникла в связи с появлением у людей методов коммуникации и осознанием того, что посредством этих коммуникаций вред может быть нанесен самим людям [8]:

По мнению отечественного ученого А. Расулева [9], следует различать следующие этапы развития информационной безопасности:

Первый этап — этап первичного осознания опасности киберпреступлении (1970 —

Т. 8. №12. 2022
https://doi.org/10.33619/2414-2948/85

конец 1990 гг.). Характеризуется зарождением и развитием компьютерной преступности, а именно первыми фиксируемыми официально фактами использования компьютеров для совершения других преступлений, как правило, мошенничеств и краж финансов, и постепенным технологическим развитием компьютерной инфраструктуры, появлением, так называемых хакеров, кракеров и прочих лиц, совершающих компьютерные преступления в виде взломов, компьютерных саботажей.

Важнейшим событием в исторической ретроспективе развития международно-правового регулирования информационной безопасности стало принятие концепции нового международного информационного порядка (НМИП).

Дальнейшее развитие регулирования в сфере обмена информацией было связано с развитием космических спутников, когда телевещание стало выходить на новый уровень. Все это привело к определенным международным проблемам, которые следовало решать. В связи с этим в 1982 году принимается резолюция Генеральной Ассамблеи ООН 37/92 «Принципы использования государствами искусственных спутников Земли для международного непосредственного вещания, а также принимается Декларация руководящих принципов ЮНЕСКО по использованию вещания через спутники для свободного распространения информации и расширения культурных обменов 1972 года и пр.».

Основной проблемой, которую пыталось решить международное сообщество указанными выше документами, была пробелам суверенитета государств, на территорию которых происходило вещание через спутники. Дело в том, что когда такое вещание информации противоречит идеологии государства или его политическим основам, то это будет уже вмешательством во внутренние дела суверенного государства. Следовательно, такая деятельность должна учитывать суверенные права каждого государства включая принцип невмешательства. Вещание через спутник должно быть свободным от политических идеологий.

Представляется, что вещание через спутник пусть даже и телевизионного сигнала, тесно связано с распространением информации в рамках информационного пространства в современном его понимании. Таким образом, так или иначе, но происходит распространение той или иной информации через государственные границы суверенных государств.

В науке международного права на основе анализа существующих тогда документов в сфере информационной безопасности выделили такие основные принципы:

– деятельность в сфере телевещания должна способствовать распространению информации в области культуры, науки, должна способствовать взаимному обмену ими, содействовать развитию образовательной среды, что в целом должно приводить к повышению качестве жизни народов и обеспечивать им досуг при уважении политической и культурной ценности каждого государства;

– все государства вправе заниматься деятельностью по телевещанию и вправе использовать блага от осуществления такой деятельности. Доступ к технологиям в данной сфере должен быть открытым для всех без исключения государств, без какой-либо дискриминации на взаимно согласованных условиях;

– деятельность в сфере телевизионного вещания при помощи спутников должна быть основана на международном сотрудничестве;

– государства несут международную ответственность за деятельность в сфере международного телевизионного вещания при помощи спутников, которое они осуществляют под своей юрисдикцией [10].

Второй этап — этап развития глобальной информационной безопасности (конец 1990

Т. 8. №12. 2022
https://doi.org/10.33619/2414-2948/85

— начало 2010 гг.). Характеризуется глобализацией и «интернационализацией» компьютерной преступности, признанием данного вида преступности в качестве глобальной угрозы — киберпреступности, дальнейшим усилением вызовов и возникновением угроз против информационной безопасности, стремительным технологическим прорывом, созданием новых информационно-коммуникационных систем и инфраструктуры, так называемого «виртуального пространства», создающего огромные возможности для трансграничного совершения киберпреступлений, активным развитием хакерских сообществ, их прогрессирующим вовлечением в преступную сеть.

Указанный этап отличается тем, что практически все страны мира в полной мере прочувствовали опасность киберпреступлений, поэтому с той или иной степенью успешности в разных странах принимаются законы, устанавливающие ответственность за различные виды преступлений в сфере компьютерной информации. Следует в этой связи подчеркнуть, что именно в этот период в Уголовном кодексе Республики Узбекистан 1994 года появилась статья 174 «Нарушение правил информатизации». В свою очередь, в 2007 году была принята специальная глава, содержащая шесть статей, устанавливающих ответственность за преступлениями в сфере информационных технологий (https://lex.uz/docs/111457).

Глобальный масштаб обретает работа по созданию механизмов межгосударственного сотрудничества в борьбе против киберпреступности. В частности, в 2000–2010 годах было принято более 20 международных актов, на глобальном и региональном уровнях, устанавливающих конкретные механизмы унификации соответствующих норм уголовного законодательства стран, а также правила юрисдикции по расследованию данных преступлений, имеющих трансграничный характер.

В частности, в 2000 принимается конвенция ООН против транснациональной организованной преступности, установивший перечень правонарушений в сфере компьютерных технологий, а также порядок межгосударственного сотрудничества по вопросам обмена правовой информацией. Стоит отметить, что в настоящее время Республика Узбекистан в области противодействия киберпреступности ратифицировала лишь Конвенцию ООН против транснациональной организованной преступности (Постановление Олий Мажлиса Республики Узбекистан от 30 августа 2003 года №536–II).

Третий этап — современный этап (с 2010 года по настоящее время). Трансформация киберпреступности в преступления в сфере информационных технологий и информационной безопасности, превратившихся в мощный системный инструмент межгосударственного, межнационального и межструктурного противоборства, который характеризуются усилением информационных атак, представляющих собой совершенно новый вид информационных вызовов, создающих угрозу не только личности, обществу или государству, но и человеческой цивилизации в целом.

На текущий период было принято около 10 международных актов, в которых регламентировались различные аспекты использования сети Интернет и создания глобальной культуры кибербезопасности. При этом обеспечение кибербезопасности было указано в качестве важнейшей и приоритетной гарантии достижения международной стабильности. Действительно, вопросы обеспечения информационной безопасности и противодействия киберпреступлениям требуют усилий не только отдельных стран, но международных организаций и мирового сообщества. Именно поэтому, на наш взгляд, возникает необходимость принятия в рамках ООН новой Конвенции по противодействию киберпреступности и обеспечению кибербезопасности, которая по своему содержанию и масштабу правового регулирования и применения будет носить универсальный характер,

Т. 8. №12. 2022
https://doi.org/10.33619/2414-2948/85

учитывать интересы всех стран мира и реалии сегодняшнего дня.

Таким образом, можно сделать следующие выводы:

Информационную безопасность можно определить, как специфическое состояние общества, при котором обеспечена всеобъемлющая защита личности, общества, государства и международного сообщества в реальном и виртуальном информационном пространстве от воздействия на них специфических угроз, выступающих в форме организованных или стихийно возникающих внутренних и внешних информационно-коммуникационных потоков.

Международно-правовое регулирование информационной безопасности исторически начиналась не с самой информационной безопасности в современном ее понимании, а в большей степени относилось к вопросам содержания информации, которая передается. Концепция нового информационного порядка была первой попыткой международно-правового регулирования в целом информационных отношений.

Развитие информационных технологий привело к возникновению общественных отношений, которые стали оказывать влияние на международное сообщество в целом. В США, а затем и в Европе к концу прошлого века начинают принимать документы, касающиеся непосредственно информационной безопасности, в частности, которые в большей части касались компьютерных систем и информации, которая передается при их помощи.

Важным и, пожалуй, одним из главных механизмов обеспечения информационной безопасности является механизм сотрудничества суверенных государств в борьбе с информационным терроризмом и информационной преступностью в целом.

Список литературы:

1. Нугманов Н. А. Международно-правовые аспекты обеспечения информационной безопасности государства. Ташкент: УМЭД, 2012.

2. Стрельцов А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы. М.: МЦнМО, 2002. 290 с.

3. Кисляковский А. В. Административно-правовое обеспечение информационной безопасности: дис. ... канд. юрид. наук. М., 2003.

4. Dunn M. A. Securing the digital age: the challenges of complexity for critical infrastructure protection and IR theory // International Relations and Security in the Digital Age. Routledge, 2007. P. 105-125.

5. Eriksson J., Giacomello G. (ed.). International relations and security in the digital age. London : Routledge, 2007. V. 52.

6. Nye J. S. The future of power. Public Affairs, 2011.

7. Доклад Генеральной Ассамблеи ООН A/55/40, 10 июля 2000; A/55/140/Add. 1, 3 октября 2000 // Информационные вызовы национальной и международной безопасности. М., 2001. 315 с.

8. Крутских А. В. Международная информационная безопасность: теория и практика. М.: Аспект- Пресс, 2019. Т. 1. Гл. 1. С 16.

9. Расулев А. К. Совершенствование уголовно-правовых и криминологических мер борьбы с преступлениями в сфере информационных технологии и безопасности. Ташкент: Академия МВД, 2018.

10. Пащенко И. Ю. О международных и внутригосударственных правовых аспектах обеспечения информационной безопасности // Новый университет. Серия: Экономика и право. 2015. №7 (53). С. 106-108.

References:

1. Nugmanov, N. A. (2012). Mezhdunarodno-pravovye aspekty obespecheniya informatsionnoi bezopasnosti gosudarstvayu. Tashkent. (in Uzbek).

2. Strel'tsov, A. A. (2002). Obespechenie informatsionnoi bezopasnosti Rossii. Teoreticheskie i metodologicheskie osnovy. Moscow. (in Russian).

3. Kislyakovskii, A. V. (2003). Administrativno-pravovoe obespechenie informatsionnoi bezopasnosti: dis. ... kand. yurid. nauk. Moscow. (in Russian).

4. Dunn, M. A. (2007). Securing the digital age: the challenges of complexity for critical infrastructure protection and IR theory. In *International Relations and Security in the Digital Age* (pp. 105-125). Routledge.

5. Eriksson, J., & Giacomello, G. (Eds.). (2007). *International relations and security in the digital age* (Vol. 52). London: Routledge.

6. Nye, J. S. (2011). *The future of power*. Public Affairs.

7. Doklad General'noi Assamblei OON A/55/40, 10 iyulya 2000; A/55/140/Add. 1, 3 oktyabrya 2000 (2001). Informatsionnye vyzovy natsional'noi i mezhdunarodnoi bezopasnosti. Moscow. (in Russian).

8. Krutskikh, A. V. (2019). Mezhdunarodnaya informatsionnaya bezopasnost': teoriya i praktika. Moscow. (in Russian).

9. Rasulev, A. K. (2018). Sovershenstvovanie ugolovno-pravovykh i kriminologicheskikh mer bor'by s prestupleniyami v sfere informatsionnykh tekhnologii i bezopasnosti. Tashkent. (in Uzbek).

10. Pashchenko, I. Yu. (2015). O mezhdunarodnykh i vnutrigosudarstvennykh pravovykh aspektakh obespecheniya informatsionnoi bezopasnosti. *Novyi universitet. Seriya: Ekonomika i parvo,* (7 (53)), 106-108. (in Russian).

Работа поступила
в редакцию 09.11.2022 г.

Принята к публикации
17.11.2022 г.

Ссылка для цитирования:

Бердимуратова Г. М. Вопросы обеспечения информационной безопасности в международном праве // Бюллетень науки и практики. 2022. Т. 8. №12. С. 434-440. https://doi.org/10.33619/2414-2948/85/52

Cite as (APA):

Berdimuratova, G. (2022). Issues on Ensuring Information Security in International Law. *Bulletin of Science and Practice, 8*(12), 434-440. (in Russian). https://doi.org/10.33619/2414-2948/85/52