ИНФОРМАЦИОННЫЙ АСПЕКТ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

М.В. Петров, *студент*
Научный руководитель: *И.Р. Аминов, канд. юрид. наук, доцент*
Уфимский университет науки и технологий
(Россия, г. Уфа)

DOI:10.24412/2500-1000-2023-1-3-69-72

Аннотация. *Сегодня, когда наше общество становится все более цифровизированным, мы можем воочию увидеть все те угрозы, которые несет данный процесс, а также можем заметить и то, как некоторые государства или опасные группировки используют данную тенденцию в целях, противоречащих принципам сохранения мира и безопасности. В данной научной статье рассмотрены некоторые аспекты международной информационной безопасности, а также явления и действия государств, которые угрожают этой системе и общей стабильности человечества.*

Ключевые слова: *международная безопасности; информационное оружие; информационные войны; терроризм.*

Научно-технический прогресс в последние два века существования человечества стал одним из основных аспект развития общества. Сегодня мы уже не можем представить себе мир без компьютеров, смартфонов и прочих благ цифровой эпохи, которые значительно облегчают нам жизнь и проникают во все сферы жизни общества. И, как ни странно, многие из современных гаджетов используются именно для распространения информации. Массовое распространение новейших средств коммуникации и глобализация информационного пространства предоставили доступ различным террористическим и экстремистским к легким путям пропаганды деструктивных идей в информационном пространстве государств. Это, без всякого сомнения, является прямой угрозой национальным интересам отдельных государств, а также всему мировому сообществу [1].

Кроме того, появляется так называемое информационное оружие, которое, используется в рамках информационных войн. Информационная война в свою очередь – война нового типа, принципы информационных войн были сформулированы уже в прошлом веке. Информационные войны представляют собой противодействие государств в информационной сфере, то есть в целом, исключает прямое столкновение, но при этом, угроза от информационного оружия исходит вполне сопоставимая, если не большая, чем от обычного оружия и традиционных войн. Концепция информационной войны используется государствами для оказания психологического влияния на население противоборствующей страны, а также дестабилизации социальной или политической ситуации. Соединенные Штаты, например, ведут информационные войны против Китая, и, особенно, России. Так, как в России, в отличии от Китая куда более либеральное законодательство в рамках вопроса о регуляции работы СМИ и Интернета [2].

Особенно ярко применение технологий информационной войны проявилось во время Специальной Военной Операции, когда большинство пророссийских международных СМИ были практически полностью ликвидированы, а их вещание серьезно ограничено или вовсе запрещено некоторыми государствами, например, Латвией. Тем самым, информационные ресурсы коллективного Запада получили монополию на освещение действий России на Украине в необходимом именно им ключе.

В рамках «Информационных войн» кроме всего прочего используются и так называемые психологические операции, а также создаются специальные подразделения в армиях государств мира, которые занимаются проведением данных операций. Они также призваны к организации

дестабилизации среди населения противоборствующих государств. Кроме того, очевиден и тот факт, что современное использование СМИ для распространения «фейков», особенное в рамках СВО, также является частью «психологических операций» [3].

Из всего описанного выше, можно сделать вывод, что в целом, международная система информационной безопасности вещь крайне хрупкая, а если мы посмотрим на определение данного понятия, которое сформулировано следующим образом: международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве. Из определения мы можем сделать вывод, что на данный момент международная информационная безопасность, увы находится в достаточно неустойчивом состоянии, однако, существование подобной системы необходимо для того, чтобы установить состояние международного мира и безопасности не только в информационном пространстве, но и «оффлайн». Однако, большинство государств не стремятся к установлению международной информационной безопасности, в виду постоянно продолжающихся «информационных войн», «психологических операций» и т.д. Не стоит забывать и о том, что, как сказано выше, дестабилизируют информационное пространство не только действия государств, но и террористические группировки, которые, с помощью современных технологий значительно расширяют их сферу деятельности и количество потенциальных последователей деструктивных идеологий по всему миру [4].

Тем не менее, попытки создать систему международной информационной безопасности предпринимаются, так, как государства все же осознают определенную угрозу, которая исходит от глобализации информационного пространства и недобросовестного использования информационных технологий. С этой целью, государства и международные государства создают документы и конвенции, а также сотрудничают друг с другом для дальнейшего развития международной информационной безопасности [5].

Например, в концепции Конвенции ООН об Обеспечении Международной Информационной Безопасности отмечены следующие принципы обеспечения информационной безопасности:

1. Совместимость с задачами поддержания международного мира, безопасности и стратегической стабильности.

2. Соответствие общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы в международных отношениях, невмешательства во внутренние дела других государств, уважения суверенитета государств, основных прав и свобод человека.

3. Неделимость безопасности, означающая, что безопасность каждого государства неразрывно связана с безопасностью всех других государств и должна обеспечиваться без ущерба безопасности других государств.

4. Достаточность потенциала любого государства по обеспечению безопасности национального информационного пространства.

5. Суверенное равенство и одинаковые права, а также одинаковые обязанности государств независимо от различий экономического, социального, политического или иного характера.

6. Возможность установления суверенных норм и механизмов управления своим информационным пространством в соответствии с национальными законами.

7. Свобода и самостоятельность в реализации своих суверенных интересов в информационной сфере, а также свобода в выборе способов обеспечения собственной информационной безопасности в соответствии с международным правом.

8. Урегулирование конфликтов путем переговоров, посредничества, примирения, обращения к профильным региональным органам или иными мирными средствами по своему выбору таким образом, чтобы не подвергать угрозам международный мир и безопасность.

9. Применимость неотъемлемого права на самооборону перед лицом агрессивных действий в информационном пространстве при условии достоверного установления источника агрессии и адекватности ответных мер с учетом норм международного гуманитарного права.

10. Недопустимость бездоказательных и необоснованных обвинений других государств в совершении противоправных деяний с использованием информационно-коммуникационных технологий, включая компьютерные атаки, в том числе для последующего принятия различного рода наказаний в виде санкций и иных способов реагирования.

11. Соблюдение основных прав и свобод граждан, включая защиту от несанкционированного вмешательства в частную жизнь граждан, и соблюдение при этом баланса между этими правами и задачами противодействия использованию информационного пространства в террористических и иных преступных целях.

12. Недопустимость ограничений или нарушений доступа к информационному пространству кроме как в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

13. Недопустимость трансграничного доступа к компьютерной информации, хранящейся в информационной системе другого государства, без официального взаимодействия с правоохранительными органами данного государства.

14. Добровольность и взаимность в деятельности по предупреждению, выявлению, пресечению, раскрытию и расследованию противоправных деяний в сфере использования информационно-коммуникационных технологий, в том числе в террористических и иных преступных целях, и ликвидации последствий таких деяний.

Из указанного выше, мы можем сделать вывод, что хотя обеспечение информационной безопасности и осложнено рядом факторов, которые включают, в основном, противодействие государств в информационном пространстве, тем не менее, государства осознают необходимость сотрудничества в сфере МИБ, для борьбы с деструктивными идеями и явлениями современного общества. Создание устойчивой системы МИБ вполне возможно, однако, это потребует значительных усилий государств-участников мирового сообщества, а также прекращения масштабных информационных противостояний.

Библиографический список

1. Жилкина Ю.В. Международная безопасность в эпоху глобализации мировой экономики // Национальные интересы: приоритеты и безопасность. – 2010. – №25. – С. 62-68.

2. Панарин И.Н. Информационная война, PR и мировая политика. – М.: Горячая Линия – Телеком, 2006. – С. 150-152.

3. Валиахметова Г.Н. Проблемы информационной безопасности в Азии // Известия Уральского федерального университета. – 2015. – № 1 (137). – С. 128-136.

5. Баришполец В.А. Информационно-психологическая безопасность: основные положения // Радиоэлектроника. Наносистемы. Информационные технологии. – 2012. – № 5. – С. 62-104.

6. Еркин А.В. Понятия «информация» и «информационная безопасность»: от индустриального общества к информационному // Информационное общество. – 2012. – №1. – С. 68-74.

INFORMATION ASPECT OF INTERNATIONAL SECURITY

M.V. Petrov, *Student*
Supervisor: *I.R. Aminov, Candidate of Legal Sciences, Associate Professor*
Ufa University of Science and Technology
(Russia, Ufa)

Abstract. *Today, when our society is becoming more and more digitalized, we can see firsthand all the threats that this process carries, and we can also notice how some states or dangerous groups use this trend for purposes contrary to the principles of preserving peace and security. This scientific article examines some aspects of international information security, as well as phenomena and actions of states that threaten this system and the overall stability of mankind.*

Keywords: *international security; information weapons; information wars; terrorism.*