Секция «Актуальные проблемы и тенденции правового регулирования в сфере государственного и муниципального управления»

Субъекты международной информационной безопасности

Научный руководитель – Попова Светлана Сергеевна

Шилыковская Юлия Альбертовна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Факультет государственного управления, Москва, Россия
E-mail: jsk08y@mail.ru

Степень влияния на международную обстановку информационно-коммуникационных технологий проявляется все сильнее. Для обеспечения стабильности и безопасности крайне важно уделить особое внимание вопросу субъектного состава. Несмотря на многолетнюю деятельность экспертов в данной области, общепринятый перечень субъектов все еще не утвержден. Одной из основных причин является скорость развития информационно-коммуникационных технологий и, как следствие, постоянная динамика их изменения.

Рассмотрим существующие в настоящие дни субъекты международной информационной безопасности, условно разделив их на две категории: представляющие угрозы и отражающие угрозы, основываясь на специфике осуществляемой субъектами деятельности. Первый тип выступает источником угроз, а второй - выполняет деятельность по их предупреждению и предотвращению.

Первый субъект – государства, которые являются ключевыми акторами в вопросе обеспечения международной информационной безопасности. На данный момент государства ведут деятельность по наращиванию как оборонительного, так и наступательного потенциала. Указанная деятельность осуществляется посредством выполнения своих функций и задач определенными государственными органами, их структурными подразделениями и группами аффилированных с государством субъектов. Говоря про роль органов государственной власти, отметим, что участие в реализации поставленных целей участвую исполнительные и законодательные органы: одни работают над разработкой правовых основ в области информационной безопасности, а вторые осуществляют действия по обеспечению исполнения данных основ. Наращивание информационного потенциала в информационной сфере делает государства более авторитетными и влиятельными. Это связано с тем, что у развитых государств появляется возможность осуществлятьшпионаж и распространять вредоносные программы, воздействие которых ориентированно на критические инфраструктуры. Показательным примером является разработка компьютерного вируса Stuxnet, который позволил значительно замедлить ядерную программу Ирана.

В качестве субъектов, аффилированных с государством, видится целесообразным выделить СМИ. Их особенность заключается в том, что именно они в большинстве случаев отвечают за ведение информационной войны: искажение информации с целью дезинформации лиц или попытка поменять сложившееся мышление, видение и отношение к какому-либо государству или конкретной ситуации. В действительности в последнее время значение информационных войн возрастает, при этом их характерной особенностью остается отсутствие видимых разрушений и постепенное внедрение дезинформации в различные сферы общественно-политической жизни для их дальнейшей модификации.

Возвращаясь к вопросу о субъектах, сделаем акцент на квазинезависимых структурах, которые позиционируются, как неправительственные, но на самом деле финансируются и управляются государствами. Ярким примером подобных организаций является «Сирийская гражданская оборона», известная также как «Белые каски». Данная организация

в 2013 – 2018 годах финансировалась США и занималась спасением мирных жителей, оказанием им медицинской помощи в ходе ведения боевых действий. Большой резонанс и основание для включения в субъекты международной информационной безопасности послужил ряд ситуаций, связанных с фальсификацией данных, размещаемых этой организацией в информационных сетях.

Говоря о государстве, как о субъекте международной информационной безопасности, нельзя умалять его возможность объединения с иными такими же субъектами. В результате этого объединения предполагается возникновение международных организаций, военных альянсов. В качестве примера такого субъекта можно рассмотреть НАТО. Фактом осуществления деятельности в информационной сфере выступает использование НАТО средств массовой информации для формирования негативного отношения к Российской Федерации, которое препятствует разрешению спорных ситуаций и служит показателем ведения дискриминационной политики в отношении страны.

Следующий субъект международной информационной безопасности – террористические организации. В настоящие дни все чаще информационно-коммуникационные технологии используются в качестве инструмента для осуществления пропаганды терроризма и привлечения лиц к совершению террористической деятельности. Преимуществом такого подхода является возможность выйти на глобальную аудиторию и распространить свои взгляды, идеи в условиях отсутствия цензуры. Ярким примером тому служит Крайстчерчскийинцидент: совершение террористического акта с расстрелом порядка 100 человек во время пятничной молитвы 15 марта 2019 года. Важным фактором в данной ситуации являетсяведение террористом прямой трансляции своих действий в одной из социальных сетей, что стало дополнительным средством распространения идей преступника.

Преступники и преступные группы – следующий субъект международной информационной безопасности, который необходимо рассмотреть. Информационная революция расширяет возможности совершения противоправных деяний и способствует появлению новых инструментов для их реализации. Более того, внедрение биометрии, оцифровка всей экономической и социальнойсферы, помимо очевидных преимуществ, чревато для общества и государства еще и угрозой стать уязвимее. Одним из ярких примеров совершения преступного деяния с использованием информационно-коммуникационных технологий является кибератака Colonial Pipeline – крупнейшей трубопроводной системы США, которая произошла 7 мая 2021 года. Атака заключалась во вмешательстве вредоносного ПО в работу данной трубопроводной системе. В результате данного вмешательства произошла остановка работы всех трубопроводов на 5 дней. Ущерб от произошедшего был настолько велик, что президент Дж. Байден был вынужден объявить чрезвычайное положение. Отметим, что спецификой подобных преступлений является их трансграничный характер и сложность идентификации источника противоправного деяния в условиях анонимности информационного пространства.

Помимо всего вышеуказанного, к субъектам необходимо отнести личность и общество в целом. Это видится необходимым, поскольку именно люди являются потребителями информации, которая распространяется посредством информационных сетей и систем.

Таким образом, общепринятая классификация субъектов международной информационной безопасности на данный момент отсутствует. Однако, все субъекты условно могут быть поделены на две группы: первая включает в себя субъекты, призванные обеспечить международную информационную безопасность и предупредить, предотвратить угрозы, а вторая – субъекты, создающие угрозу международной информационной безопасности. Примечательно, что порой субъекты могут быть отнесены к обеим группам одновременно в зависимости от осуществляемых ими действий.

Источники и литература

1) Резолюция Генеральной Ассамблеи ООН A/RES/53/70 от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // [Электронный ресурс]: https://digitallibrary.un.org/record/262268?ln=ru (дата обращения: 11.02.2024).
2) Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности // Право и управление. XXI век. 2014. Т. 33. № 4. С. 44-52.
3) Манойло А.В. Объекты и субъекты информационного противоборства // Пси-фактор, 2003.