

Международная информационная безопасность: проблемы и перспективы развития

Научный руководитель – Окунь Александр Борисович

Патидинов Акмалдин Вахиджанович

Студент (бакалавр)

Самарский национальный исследовательский университет имени академика С.П.

Королева, Социально-гуманитарный институт, Самара, Россия

E-mail: akmalpat@gmail.com

Современный этап развития общества характеризуется совершенствованием информационных технологий и созданием глобального информационного пространства. Председатель КНР Си Цзиньпин отметил[1], что в наши дни национальная безопасность невозможна без её кибербезопасности, а модернизация страны невозможна без её информатизации. Как и всякое явление, эти процессы имеют свои негативные стороны. Развитые страны с высоким уровнем цифровизации многих сфер жизнедеятельности общества часто попадают в ловушку своей технологичности. Чем шире применяются ими информационные технологии и чаще используют глобальную сеть, чем сложнее их информационная инфраструктура, тем ниже защищенность от кибератак и выше причиняемый ущерб. Угрозы в цифровой сфере сегодня – один из наиболее серьезных вызовов международному миру и безопасности.

Актуальность темы обусловлена тем, что информационно-коммуникационные технологии (ИКТ) все чаще используются как инструмент военно-политического давления, вмешательства во внутренние дела государств, нанесения экономического ущерба. Набирает обороты гонка информационных вооружений. Растет уровень информационной преступности, причем под корыстные преступления нередко маскируется решение политических задач.[3,4]

Быстрое развитие информационных технологии приводят к тому, что огромное количество денег, потраченных на оборонную промышленность, не смогут оправдать себя, если будет достаточно просто запустить компьютерный вирус и разрушить всю систему оборонной промышленности страны.

Наличие таких потенциальных угроз подталкивают страны на укрепление своей информационной безопасности любыми способами, даже путем создания информационного вооружения, что приводит нас к новой холодной войне.

Международное сотрудничество в области обеспечения информационной безопасности на мировом уровне усложняется и противоречиями в государственных интересах. Одним из основных причин отсутствия универсального документа по контролю деятельности стран в информационном пространстве, является отсутствие общего определения информационной безопасности. Дальнейшее формирование глобального режима, направленного на обеспечение безопасности в информационной сфере, определяется позициями наиболее влиятельных стран-участников переговорного процесса. Ключевыми субъектами сотрудничества на глобальном уровне являются Соединенные Штаты Америки, Российская Федерация и Китай. Именно эти страны обладают наибольшим потенциалом в данной сфере. Постепенное ухудшение отношения трех ведущих стран в информационной сфере приводит к росту напряженности в этой области и стимулирует остальные страны вступать в гонку кибервооружений. [2,3]

Несостоятельность ведущих стран мира создать единые правила дорожного движения в информационном пространстве приводит к хаосу. Отсутствием единых норм и правил

некоторые страны уже давно пользуются, например, запускают компьютерные вирусы, разрушающие изнутри всю оборонную систему другой стороны, или преследуют граждан других стран и крадут личные данные в информационной сфере. Из-за того, что Большие Братья не могут прийти к общему знаменателю, страны, обладающие небольшим потенциалом в области технологии, а также негосударственные акторы вступают в гонку информационных вооружений. Эта ситуация привела нас к тому, что наше поколение может увидеть новую «холодную войну».

Распространение информационных вооружений способствуют тому, что увеличивается и количество киберпреступлений. Причем с каждой такой кибератакой страдает все большее количество людей в материальном плане. [2]

Ирония в том, что исследуемые страны признают, чем больше они развиваются технологически, тем уязвимее становится их национальная безопасность. Однако, и это осознание не может заставить их сесть за стол переговоров. Эти страны просто-напросто не доверяют друг к другу. США считают Россию причастной ко всем последним кибератакам по отношению к ним, тем самым ставя их на место главной угрозы для национальных интересов США, а Китай они подозревают в кибершпионаже. Россия и Китай, напротив, готовы к сотрудничеству в сфере информации, чтобы создать единые правила поведения для государств в информационном поле.

Источники и литература

- 1) Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. М., 2012. С. 763.
- 2) Ильичев И.Е. Проблемы обеспечения информационной безопасности личности, общества и государства в современной России // Наука.Теория.Практика. 2015. № 2. URL <https://cyberleninka.ru/article/n/problemy-obespecheniya-informatsionnoy-bezopasnosti-lichnosti-obschestva-i-gosudarstva-v-sovremennoy-rossii>
- 3) Первое совещание Центральной группы по информационной безопасности и информатизации. Важная речь Си Цзиньпина. URL: http://www.cac.gov.cn/2014-02/27/c_133148354.htm
- 4) The Global Think Tank // Carnegie Endowment for International Peace. URL: <https://carnegieendowment.org/about/>