Секция «Международная безопасность: новые вызовы и угрозы»

Кибервойны как новый аспект международной безопасности

Научный руководитель – Нарышкина Ольга Михайловна

Кусакин Даниил Всеволодович

Студент (бакалавр)

Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра международной безопасности, Москва, Россия

E-mail: daniilkus2012@gmail.com

Развитие и постепенное внедрение компьютерных технологий привело к формированию новой сферы обеспечения безопасности — информационной.

В государственных органах создаются и функционируют подразделения, отвечающие за противодействие и защиту от кибератак, кражи данных и обеспечению конфиденциальности информации. В России такой деятельностью занимается Управление «К» — подразделение Министерства внутренних дел России. В США — Национальное управление кибербезопасности, подразделение Управления кибербезопасности и коммуникаций Директората национальной защиты и программ министерства внутренней безопасности США.

На международном уровне сложился новый тип взаимодействия акторов — кибепротивостояние и кибервойна. Многие государства избирают этот тип взаимодействия, как способ достижения своих целей. США, Россия, Китай, Иран и КНДР — основные страны, конкурирующие в этой сфере.

Впервые методы кибервойны были использованы во время войны в Персидском заливе 1991 года, в ходе операции «Буря в Пустыне». Американские вооруженные силы смогли продемонстрировать превосходство путем использования передовой аппаратуры и данных, полученных со спутниковой связи. Эта информация позволила повысить осведомленность войск и предотвратить многие потери. В то же время стало понятно — данные, полученные в результате использования ИКТ уязвимы для шпионажа или диверсии. На данный момент ни одну систему защиты данных нельзя назвать неуязвимой от различного вида кибератак.

Несмотря на то, что природа войны остаётся той же, ИКТ стали неотъемлемой частью сбора, обработки и распространения информации на поле боя. В тоже время, одни и те же возможности, которые дают преимущество ведения боевых действий, одновременно создают определенные уязвимости, которые позволяют противникам использовать их в своих интересах. Помимо использования уязвимостей, с помощью ИКТ появилась возможность активно обращаться к методам пропаганды, дезинформации и обмана для нарушения доступа к достоверной информации.

В подобных условиях Российская Федерация выступает за разработку актуальных и соответствующих современным тенденциям международных норм в сфере обеспечения информационной безопасности и принятие их на уровне Генеральной Ассамблеи ООН. Проект, предложенный российской стороной основан на уважении государственного суверенитета и не предполагает вмешательство во внутренние дела государства, тем самым не ущемляет его прав. Однако на данный момент внедрение таких норм затруднено. Связано это с нежеланием США и союзников по НАТО отходить от решений Будапештской конвенции Совета Европы.

Источники и литература

1) Mgimo.ru: https://mgimo.ru/about/news/experts/diplomaticheskoe-nastuplenie-rossii-v-oblasti-informatsionnoy-bezopasnosti/
2) Kaspersky.ru: https://www.kaspersky.ru/about/press-releases/2015_duqu-is-back
3) Foreignpolicy.com: https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/
4) Cbaonline.org: https://csbaonline.org/