Секция «Международная безопасность: новые и традиционные вызовы и угрозы»

Гонка кибервооружений как новая угроза международной безопасности

Научный руководитель – Эпштейн Виталий Анатольевич

Пискун Анастасия Михайловна

Студент (специалист)

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Институт бизнеса и делового администрирования, Москва, Россия

E-mail: piskun.anastasiya07@gmail.com

С развитием и проникновением информационно-коммуникационных технологий во все сферы деятельности общества и государства появляются новые вызовы и угрозы, которые сопровождаются развитием национальной и глобальной информационной инфраструктуры и значительно влияют на оборонный и политический потенциал государств. В связи с этим появляется информационное или киберпространство - явление, меняющее традиционную систему национальной безопасности и международного сотрудничества. Последнии события, связанные с пандемией и переходом всех процессов в удаленный формат, это наглядно доказало, только на критическую инфраструктуру РФ было совершенно свыше 1 млрд кибератак [14].

В следствие усиления зависимости промышленных, военных технологий от информационных систем роль киберпространства как еще одного пространства для взаимодействия различных политических акторов возрастает. В результате за лидерство в этом пространстве ведется активная борьба между такими государствами как США, КНР, РФ, Израилем, Великобританией, Ираном [15]. Так, в 2010 г. заместитель министра обороны США Уильям Линн назвал позицию руководства относительного этого пространства: «Мы должны признать киберпространство тем, чем оно уже стало - новой зоной военных действий» [13], которую США намерены защищать ввиду того, что по многим параметрам США наиболее зависимое от кибертехнологий мировое государство.

Деятельность в данном пространстве влияет на все сферы современного общества: экономика и финансовый сектор, культурную и социальную сферу, активно воздействует на политические процессы. Одним из инструментов являются всевозможные технологии и программное обеспечение, которое может использоваться для разных целей, от добычи разведывательных данных до выведения из строя критически важной инфраструктуры [3]

Исходя из этого государства ведут активную разработку кибернетических вооружений, которые могут быть использованы против других государств. Специфика данного вооружения заключается в его анонимности, сложности государственного контроля, простоте распространения, а также потенциальной разрушительности, приравнивающейся к масштабам применения оружия массового уничтожения, при этом считается более эффективным и менее затратным [2]. Кроме того, практически невозможно определить точно время, когда было применено КО, т.к. его программы могут заранее проникать в сети или управляющие системы объектов КВИ и достаточно продолжительное время находиться там в спящем режиме, до тех пор, пока оно не будет приведено в действие в целях перехвата информации, управления над объектами, либо его выведения из строя и разрушения.

Военные стратеги часто сравнивают кибероружие (КО) с ядерным (ЯО) и, наравне с ЯО, называют КО оружием массового поражения, т.к. применение обоих видов может привести к колоссальным разрушениям и жертвам. Однако, если в случае ядерной войны существует система сдержек и противовесов, которая не допускает реального применения

ядерного оружия. В случае с кибернетическим оружием, четкой стратегии международного сдерживания все еще не выработано.

С каждым годом случаев проведения кибератак, применения КО и случаев шпионажа разведывательными службами растет. Правительства многих государств ведут активную работу над созданием военных киберподразделений, способов обороны и наступления в киберпространстве. Так, например, в 2010 г. после кибератаки на иранский ядерный объект в Нетензе (в рамках операции «Олимпийские игры», проведенной разведывательными службами США и Израиля против ядерной программы Ирана) руководства многих стран задумались о масштабе возможных последствий, вызванных действиями в информационном пространстве. В дальнейшем стало известно, что центрифуги на иранском заводе по обогащению урана были выведены компьютерным червем Stuxnet [3].

Если рассматривать стратегии национальной безопасности США, опубликованные в период с 2002 - по 2017 гг. [6, 7, 8], направленные на защиту интересов государства как на своей территории, так и на мировой арене, можно сказать, что вопрос применения данного вида вооружения рассматривается достаточно подробно. Только в период президентских сроков Б. Обамы сформулирована политика «киберсдерживания» и официально закреплена возможность применения наступательного кибероружия в случаях угрозы национальным интересам США [9, 10], а основными положениями Киберстратегии Д. Трампа стали защита интересов американского народа, усиление киберпотенциала США, возможность применения всех возможных инструментов для предотвращения любых киберугроз, а также усиление собственного влияния в киберпространстве, за счет создания сильного боевого Киберкомандования [11, 12].

Источники и литература

1) Буряк В. В. Цифровая экономика, хактивизм и кибербезопасность: Монография / В. В. Буряк. – Симферополь: ИП Зуева Т. В., 2019.
2) Ларина Е. С. Кибервойны XXI века: о чем умолчал Эдвард Сноуден / В. С. Овчинский, Е. С. Ларина. - М.: Книжный мир, 2014.
3) Овчинский В. С. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В. С. Овчинский. – М.: Норма, 2017.
4) Кардава Н. В. Киберпространство как новая политическая реальность. / Н. В. Кардава // История и современность. – 2018.
5) Clarke R. A., Knake R. K. Cyberwar. The Next Threat to National Security and What to Do About It / R. A. Clarke, R. K. Knake. - Ecco. - Reprint edition. - August 5, 2011.
6) The National Strategy to Secure Cyberspace. // Official website of the Department of Homeland Security, February 2003.
7) The National Strategy for Homeland Security // Homeland security council, October 2007.
8) National Security Presidential Directive (INSPD-54) / Homeland Security Presidential Directive (HSPD-23) // The White House, Washington, January 8, 2008.
9) Sustaining U.S. Global Leadership: Priorities for 21st Century // The Department of Defense, February, 2012.
10) Cyber Strategy // The Department of Defense, April 2015.
11) National Security Strategy of the United States of America // The White House, Washington, December, 2017.

12) Cyberspace Solarium Commission. March 2020
13) www.habr.com (IT СМИ)
14) www.tass.ru (российское информационное агентство)
15) www.russiancouncil.ru (Российский совет по международным делам)