Секция «Глобальное управление и безопасность»

Кибербезопасность в современном мире: к постановке проблемы

Цынарёва Наталья Александровна
E-mail: tsynareva.na@gmail.com

Цынарёва Наталья Александровна, кандидат филологических наук, старший научный сотрудник лаборатории по изучению зарубежной печати факультета журналистики Московского государственного университета имени М.В. Ломоносова

Вопрос о Третьей Мировой войне уже вряд ли можно назвать сенсационным в наше время. Международные СМИ постоянно пишут о глобальном противостоянии, переделе мира и сфер влияния. В первую очередь речь ведется о кибервойнах, которые стали реалией сегодняшнего дня. Кибервойной называют «один из новых видов войны, основанный на современных технологиях. Это не самостоятельный вид противоборства, кибервойна всегда является составной частью информационной войны, и в целом выступает элементом полномасштабной военной кампании» [3]. Кибервойна может реализовываться как со стороны традиционных акторов международных отношений, так и со стороны нетрадиционных: неправительственных организаций, специальных группировок, в том числе террористических, отдельных личностей (хакеров). С кибервойной тесно связаны такие термины, как кибератака, кибероружие, киберугроза, киберконфликт, которые пока не имеют точного определения. Некоторые исследователи градуируют степень напряженности взаимоотношений стран накануне кибервойны, выделяя начальный этап – отдельные кибератаки, совершенные при помощи определенного кибероружия; следующий этап – киберконфликт, возникающий как напряженная ситуация между 2-мя и более сторонами, обменивающимися взаимными киберугрозами; финальным этапом такого противостояния будет начало кибервойны, которая ведется незримо и незаметно. Несмотря на то, что кибервойна как явление возникло совсем недавно, уже сформировалось противоположное понятие – кибербезопасность, которое подразумевает разработку определенной системы противостояния угрозам в киберпространстве и оперативного реагирования в случае реализации подобных угроз. Впервые о кибербезопасности заговорили еще в конце 1990-ых гг., когда Россия предложила США разработать общий документ по вопросам информационной безопасности [1: 120]. Проект документа остался на уровне обсуждения, но вопрос был поставлен на международной повестке дня. В дальнейшем в 1998 году тема информационной безопасности актуализировалась на заседании Генеральной Ассамблеи Организации Объединенных Наций. В результате обсуждения возможных подходов к новому понятию была принята итоговая резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [7]. Сегодня практически все страны мира имеют собственные концепции и программы по охране киберпространства и защите данных граждан [13, 14]. В РФ этот вопрос до сих пор находится в стадии обсуждения [6]. Проект «Стратегии кибербезопасности РФ» начал разрабатываться Временной комиссией по развитию информационного общества Совета Федерации РФ еще в 2012 году [4], в конечном счете, общественности был представлен только проект «Концепции Стратегии кибербезопасности РФ» [5], не получивший дальнейшей реализации. Как выяснила газета «Коммерсант», опросив представителей органов исполнительной власти, предложенная концепция «противоречит госполитике России в данной сфере» [11]. Таким образом, вместо единого комплексного документа по информационной безопасности в России существует ряд отдельных правовых актов, частично покрывающих или ограничивающих данную область. В 2016 году была принята «Доктрина информационной безопасности Российской Федерации» [2]. Вместе с тем, в мире постоянно возникают киберугрозы, заставляющие задуматься не только о национальной кибербезопасности, но и

об общемировой стабильности и защищенности от кибератак. Первым случаем применения кибероружия называют взрыв на стратегически важном для СССР объекте – сибирском газопроводе «Уренгой – Сургут – Челябинск», который произошел в 1982 г. [3]. В период Холодной войны он был воспринят как диверсия на Советский Союз со стороны Соединенных Штатов Америки. Следующая атака была проведена в конце 1990-ых гг. и получила название «Лабиринт лунного света». Атака была направлена на серверы НАСА и Министерства обороны США. Главным источником угрозы был назван Китай, который один из первых осознал действенность и эффективность подобного оружия в современном мире. А первой кибервойной называют серию атак на «электронное правительство» Таллина, предпринятую в 2007 году в связи с решением эстонского руководства о переносе памятника Воину-освободителю. Обвинения в проведенных атаках были высказаны в адрес России, которая на данный момент, наряду с Китаем, считается одним из главных кибераграссоров в мировом киберпространстве. Впоследствии в 2013 г. Североатлантический альянс НАТО по инициативе Эстонии разработал «Таллинское руководство по ведению кибервойн», в котором были прописаны алгоритмы действий в случае массовых кибератак с учетом существующих киберугроз. В последнее время технологический прорыв настолько сильно изменил окружающую реальную и виртуальную действительность, что летом 2016 года «НАТО официально признала киберпространство потенциальным «полем боя». Ранее к таковым альянс относил сушу, воду, воздух и космос. Теперь к ним добавилось пространство, созданное человеком» [8]. Многие российские и зарубежные журналисты и исследователи открыто называют события сегодняшнего дня латентно ведущейся III Мировой войной, или I Мировой кибервойной [8, 9, 10, 12]. Страны разрабатывают концепции кибернападений, утверждают стратегии кибербезопасности и наращивают потенциалы кибервооружений. Главная проблема, встающая перед мировой общественностью, - отсутствие норм и предписаний по ограничению противоправных и разрушающих действий агрессоров в отношении разных акторов международных отношений в киберсреде.

Список литературы: 1. Бедрицкий А.В. Международные договоренности по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. № 4(13). С. 119-136. 2. Доктрина информационной безопасности РФ (от 05.12.2016) // Российская газета. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html 3. Капто А.С. Кибервойна: генезис и доктринальные очертания // Вестник Российской Академии Наук. 2013. Т. 83. № 7. С. 616-625. 4. Концепция Стратегии кибербезопасности. Интервью // Вопросы кибербезопасности. 2014. № 1(2). URL: http://cyberrus.com/wp-content/uploads/2014/03/2-4.pdf 5. Концепция Стратегии кибербезопасности РФ. Проект. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf 6. Пуля В. Суверенная кибербезопасность: как глобальные проблемы влияют на ограничения медиа в интернете // MediaToolbox. 09.02.2015. URL: http://mediatoolbox.ru/blog/suverennaya-kiber-bezopasnost-kak-globalnyie-problemyi-vliyayut-na-ogranicheniya-media-v-internete/ 7. Резолюция ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Организация Объединенных Наций. URL: http://www.un.org/ga/search/view$_doc.a$
$A/RES/53/70referer = /english/Lang = R8..//Globalaffairs.29.11.2016.URL : http :$
$//www.globalaffairs.ru/number/Nachalo-kholodnoi-kibervoiny-184889..//Globalaffairs.09.1$
$http : //www.globalaffairs.ru/global - processes/Politicheskaya - kibervoina - nachalas -$
$1841510..//Globalaffairs.23.09.2016.URL : http : //www.globalaffairs.ru/global-processes/Sm$
$li-derzhavy-dogovoritsya-o-pravilakh-povedeniya-v-kiberprostranstve--1838111.., .//.ru2$
$http : //www.kommersant.ru/doc/235515412.BenitezJ.LaTerceraGuerraMundialyahaestalladoy$
$http : //www.elmundo.es/papel/historias/2017/03/12/58c151f522601dab398b45dc.html13.Interna$
$http : //www.pircenter.org/media/content/files/9/13480895180.pdf14.TheDODCYBERSTRAT$
$https : //defence.ru/document/61/$