Автор: admin
24.03.2022 17:40 - Обновлено 02.07.2022 16:20

В ООН понимают, что заявления официальных лиц США и их европейских партнеров стали образцом дезинформации, цинизма и безнравственности по отношению к мировому сообществу, что не отвечает интересам поддержания мира и стабильности в сфере международной информационной безопасности. В течение второго месяца 2022 года, не смотря на проведение Олимпийских игр в Китае, как и прогнозировало независимое экспертное сообщество, накал информационной (гибридной) войны достиг критической черты.
По мнению специалистов, уровень угрозы информационной безопасности Российской Федерации от действий сил и средств в информационно-коммуникационном пространстве приближается к так называемому «периоду нарастания военной угрозы для национальной безопасности государства».

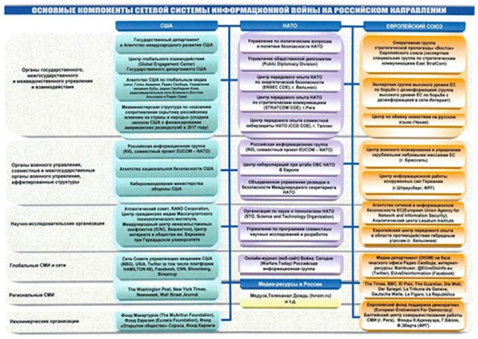
Этот период характеризуется степенью возможного нанесения ущерба национальным интересам и критически важной информационной инфраструктуре российского государства. При этом учитывается условие, что Российская Федерация располагает (сохраняет) потенциал и необходимые ресурсы для нанесения существенного или неприемлемого ущерба критически важной информационной инфраструктуре противоборствующей стороны с необходимой степенью вредоносного воздействия на систему государственного и военного управления, включая центры принятия решений. В этой ситуации главной опасностью для любого противника Соединенных Штатов является снижение президентом США порога принятия решений на проведение кибератак на критически важные объекты информационной инфраструктуры. В какой момент Пентагону придет в голову повторить атаку подобную использованию вируса Stuxnet против иранских ядерных объектов? К каким жертвам и последствиям для экологии и экономики может это все привести?

Напряженность в информационном пространстве практически целиком провоцируется сознательно и целенаправленно как безапелляционными и безответственными заявлениями западных политиков, так и обслуживающими их интересы ведущими мировыми СМИ. Так, вслед за ложью

официальных лиц разного калибра из Вашингтона о якобы «подготовке Россией фейкового видеосюжета об агрессии ВСУ на Донбассе», американское агентство Bloomberg на своем сайте разместило заголовок «Прямой эфир: Россия вторгается на Украину» («Live: Russia invades Ukraine»).

Абсурдность появления фейковой новости вынудила сделать заявление представителя Генсека ООН Фархана Хака, что «следует избегать любых действий или риторики, которые могут привести к эскалации ситуации».

До этого Bloomberg уже распространил дезинформацию о так называемой закулисной просьбе Китая к России «не нападать на Украину во время Олимпиады в Пекине». Пресс-секретарь Президента РФ Д.Песков оценил такие действия как демонстрацию того, насколько опасна ситуация, провоцируемая бесконечными агрессивными заявлениями, которые идут из Вашингтона и европейских столиц. Распространение откровенной лжи о российской военной угрозе используется длительное время для обоснования продвижения НАТО к границам РФ, роста военных расходов блока и отвлечения внимания населения от ухудшения социально-экономического положения в собственных странах.



В сентябре 2021 года на 15-м международном форуме в Москве советник Секретаря Совета Безопасности Российской Федерации, Президент Национальной Ассоциации международной информационной безопасности Владислав Шерстюк отметил, что «Евросоюз и НАТО под видом борьбы с гибридными угрозами и с дезинформацией из России открыто вбрасывают через средства массовой коммуникации грубую ложь и фейки, ведут русофобский роботроллинг в

соцсетях, используют весь кибераршенал ментальной войны против РФ и ее союзников, включая инспирирование «пятой колонны».

Основу кибервозможностей и киберпотенциала, в том числе для нанесения ущерба наиболее важным системам обеспечения жизнедеятельности государства и населения, составляют так называемые кибервойска, прежде всего США, Великобритании, Германии и Франции. В настоящее время численность киберкомбатантов в этих структурах превышает несколько десятков тысяч военнослужащих и гражданского персонала. Вышел на полноценную боевую работу Центр кибероперaций при штабе ОВС НАТО в Европе.

Анализ деструктивной вредоносной и злонамеренной деятельности глобальной многоуровневой системы информационной войны (ИВ), созданной США, их союзниками и партнерами (представлена на схеме), обуславливает необходимость принятия срочных мер на уровне ООН в интересах формирования системы международной информационной безопасности (МИБ) и обеспечения стратегической стабильности. Главной опасностью для международного сообщества является недекларируемая цель этой системы ИВ – формирование виртуальной реальности с одновременным переформатированием мирового общественного сознания под «определенные стандарты» мирового правительства (господствующей элиты).

Учитывая реальную опасность для мира, прежде всего, должен быть принят под эгидой ООН международный правовой акт (конвенция), регулирующий деятельность государств в области МИБ, созданы международная и национальные структуры управления кибербезопасностью (информационной безопасностью), а также национальные группы реагирования на компьютерные чрезвычайные ситуации (CERT) и группы реагирования на инциденты компьютерной безопасности (CSIRTs), которые могли бы полноценно противодействовать всему спектру информационных угроз. Деятельность указанных структур должна быть организована и контролироваться национальными правительствами, носить публичный и прозрачный характер с участием частного сектора и гражданского общества.

Национальные системы обеспечения информационной безопасности должны располагать потенциалом достаточным решать задачи по защите критически важной информационной инфраструктуры государства, а также для эффективного противодействия деструктивному

информационно-психологическому воздействию на общественное сознание населения путем выявления и законодательного ограничения распространения противоправного и фейкового контента. На международном уровне обсуждается целесообразность создания эффективного независимого процедурного механизма для справедливого судебного наказания за киберпреступления , в том числе за счет мер гармонизации национальных законодательств в сфере борьбы с преступлениями с использованием информационно-коммуникационных технологий.

**Таким образом, насущной проблемой в текущем столетии становится взятие мировым сообществом на себя обязательств выработки (адаптации) и соблюдения норм ответственного поведения государственных акторов в информационном пространстве, основанных на принципах Устава ООН и других норм международного права:соблюдение суверенного равенства;разрешения международных споров и противоречий мирными средствами без того, чтобы не подвергать угрозам международный мир, безопасность и справедливость;
отказ от угрозы силой или ее применения в международных отношениях.**

Коротков С.В., кандидат военных наук