О НОВОМ ЭТАПЕ ИНФОРМАЦИОННОЙ ВОЙНЫ ЗАПАДА ПРОТИВ РОССИИ

Автор: admin
14.04.2024 20:58 - Обновлено 14.04.2024 21:46

По образному выражению Министра иностранных дел России С. Лаврова «пещерная русофобия» стала приоритетной нормой в политике представителей западных элит, среди которых дошло до обсуждения вопроса непосредственного использования вооруженных сил европейских государств против российского государства.

Основные причинно-следственные факторы, обусловившие переход западной системы информационной войны к новому этапу злонамеренной и вредоносной деятельности на российском направлении

Под влиянием США наблюдается процесс дальнейшей деградации политической элиты в высших органах власти государств западного сообщества. Не лучшим образом происходит трансформация роли и работы международных организаций и их структур (ЕК, ЕС, ОБСЕ, ЮНЕСКО, ОЗХО, МОК и др.).

Неготовность Запада отказаться от заявленной цели нанести «стратегическое поражение России», с учетом не оправдывающего затраты на реализацию проекта «Украина – АнтиРоссия», вынуждает США, НАТО и ЕС усилить активные наступательные действия на новом поле войны – киберпространстве. Весомым аргументом для этого у западных специалистов в области информационного противоборства является ставка на потенциальные возможности использования нового мощного инструмента – технологий искусственного интеллекта.

Вместе с тем на проводимую Западом политику продолжают оказывать влияние результаты деятельности западных аналитических центров в виде прогнозных оценок и рекомендаций политико-формирующим кругам и органам власти в отношении России, которые оказались большей частью субъективными и конъюнктурными. В результате этого принимаемые судьбоносные управленческие решения западными лидерами на протяжении текущего столетия все более не отвечают национальным интересам и благополучию народов стран т.н. «золотого миллиарда».

Глубинными же факторами возрастания агрессивности действий Запада на мировой арене являются исторически «банальные» экономические интересы. Снижение политической роли, экономического потенциала западного сообщества, а также ограничение доступа к мировым сырьевым ресурсам вынуждают США и его союзников предпринимать попытки дестабилизировать обстановку в ряде регионов мира, инспирировать противоречия в межгосударственных объединениях и организациях с участием России. Для этой цели задействуется т.н. «глобальная система информационной войны».

Основные индикаторы, характеризующие новый этап информационной войны на российском направлении

К ряду основных индикаторов, характеризующих новый этап информационной войны на российском направлении, можно отнести следующие действия и события, имеющие место в российском (национальном) и глобальном информационном пространстве. В их числе:

- неприкрытое вмешательство во внутренние дела России с попытками повлиять на результаты выборов Президента Российской Федерации;
- злонамеренная и вредоносная деятельность США, НАТО и ЕС с использованием потенциала Украины в информационном пространстве в целях нивелирования сорванного наступления ВСУ, нанесения ущерба российской национальной критически важной информационной инфраструктуре;
- оказание англосаксами агрессивного информационного давления на союзников и партнеров в целях продолжения оказания всесторонней помощи Украине и недопущения прекращения военных действий;
- проведение демонстративных информационно-пропагандистских акций антироссийской направленности со стороны приграничных с Россией государств;
- реализация комплекса мероприятий по дискредитации России в БРИКС в период ее председательства в объединении;
- принятие США и их союзниками новых доктринальных документов и

законодательных актов в области кибербезопасности, а также инспирирование недружественных действий антироссийской направленности в ряде зарубежных стран с элементами «российской шпиономании».

Российской общественностью негативно воспринята информация СВР России о том, что администрацией президента США была поставлена задача перед подконтрольными НПО добиться снижения явки избирателей 15-17 марта 2024 г. При этом вскрыты и зафиксированы факты участия американских IT-специалистов в распространении через Интернет-ресурсы призывов к гражданам России игнорировать выборы. Данная злонамеренная деятельность ранее получила дополнительный импульс от политиков на Западе с активизацией потенциала несистемной оппозиции и агентов влияния, используя резонансный повод, связанный с фигурой оппозиционного лидера Алексея Навального, скончавшегося 16 февраля 2024 года в исправительной колонии особого режима «Полярный волк».

С начала избирательной компании 2024 года на сайт ЦИК России обрушилось 12 миллионов хакерских атак. Для сравнения стоит отметить, что на инфраструктуру систем дистанционного электронного голосования в сентябре 2023 г. злоумышленниками было совершено более 30 тысяч DDoS-атак из-за рубежа. В период онлайн-голосования во время выборов в России в сентябре 2021 года кибератаки велись с IP-адресов, зарегистрированных в разных странах, но половина всех атак – из США, а 25% - из Германии.

Одним из индикаторов вредоносной деятельности с политической и криминальной мотивацией является резко возросший объем похищенных (слитых) персональных данных.

Значительная часть компьютерных атак проводится зарубежными спецслужбами стран-членов НАТО под «чужим флагом» с использованием т.н. «ИТ-армии Украины» и аффилированных с ней «колл-центров» для совершения мошеннических действий в отношении российских граждан. Фактическим подтверждением этому является годовой отчет Агентства национальной безопасности США, в котором России отводится роль основного киберпреступника, и она заявлена как угроза «региональной безопасности и глобальной стабильности», а украинское направление подчеркнуто признано приоритетом в деятельности АНБ.

В этой связи заслуживает внимание особая роль АНБ и Киберкомандования, которые занимают ведущее место в Альянсе по обмену разведданными Five Eyes, в который входят Австралия, Канада, Новая Зеландия, Великобритания и США. С началом проведения Россией СВО и особенно в последнее время усилились обвинения России и Китая в хакерстве, что является «коллективной кампанией дезинформации» со стороны стран «Пяти глаз».

Одной из задач, проводимых США информационных операций является распространение негативной информации о социально-экономическом положении российского общества, осуществление т.н. сливов дезинформации в интересах дискредитации России в БРИКС в период ее председательства в объединении с целью посеять раздор в объединении.

Последние противоречивые заявления президента Франции Э.Макрона о возможном направлении европейских военнослужащих на Украину являются также элементом и индикатором информационной кампании, одной из задач которой просматривается моральная и идеологическая подготовка населения натовских стран и граждан Украины к вероятному разделу и оккупации остатков «Незалежной».

Примечательно, что бывший премьер-министр Франции Доминик де Вильпен призвал «общественность не устраивать бурю в стакане воды из-за воинственных заявлений Макрона…, которые правильнее было бы назвать стратегической возбужденностью или стратегической сумятицей. В целом затеять одновременно и войну, и Олимпийские игры - это чересчур амбициозные планы для страны, находящейся не в лучшей форме. Если силовое противостояние выйдет из-под контроля, то эскалация может быть смертельной».

По образному выражению официального представителя МИД России М. Захаровой «то, что предлагает президент Франции Э. Макрон – это очередной «мыльный пузырь» Елисейского дворца».

Показателем активизации информационной кампании антироссийской направленности является рост объема распространения дезинформации «недружественными странами». Продолжаются с определенной периодичностью бездоказательные обвинения России в проведении кибератак с различными целями. Так, министр обороны Франции в феврале с.г. заявил в ходе интервью «Journal du Dimanche», что объекты

французской инфраструктуры все чаще подвергаются кибератакам со стороны России. По его словам, в конце 2023 года была отражена кибератака на крупную французскую оборонную компанию. При этом он ранее назвал заявление о французских наемниках на Украине частью «российской информационной войны».

Свою «ложку дегтя» в злонамеренную деятельность вносят прибалтийские государства. Меры, которые принимаются представителями власти стран Прибалтики, свидетельствуют о том, что они являются зависимыми субъектами в качестве участников информационной войны против России. Безответственностью и политической близорукостью оцениваются слова президента Латвии Эдгарса Ринкевичса о том, что «Россия должна быть разрушена». Ранее премьер-министр Латвии Эвика Силиня торжественно провозгласила, что между Россией и странами Прибалтики появится «железный занавес».

Показательным индикатором и фактом активизации информационной войны являются меры по усиления цензуры в связи с принятием 13 марта с.г. депутатами Европарламента большинством голосов контроверсиального закона о свободе СМИ в ЕС. Закон предоставляет дополнительные полномочия Европейской комиссии для регулирования медиа пространства в странах-членах. По мнению оппозиционных евро депутатов, в частности Катрин Гризе из Франции, данный новый орган надзора (Комитет по СМИ) будет подвержен воздействию Европейской комиссии и может присвоить себе полномочия национальных органов по контролю за медиа в различных странах.

Такая оценка вполне реалистична, имея в виду, что свобода СМИ в Европейском союзе является основным правом, которое распространяется на все государства-члены Европейского союза и его граждан, как определено в Хартии основных прав ЕС, а также в Европейской конвенции о правах человека. Складывающая ся ситуация в медиа пространстве ЕС все более ограничивает свободу прессы и таким образом ограничивает свободу выражения мнений и свободу информации, нивелирует элементарную возможность выражать оценочные суждения и право утверждать факты соответственно.

Одним словом, оценить принятие евро депутатами очередного сакрального закона можно как подарок самим себе к ежегодному Всемирному дню свободы печати, который отмечается 3 мая.

Вызывает озабоченность, что ЮНЕСКО постепенно утрачивает объединительную повестку дня. По заявлению Постоянного представителя России на 217-й сессии Исполнительного комитета ЮНЕСКО «на её площадке все чаще звучат пропагандистские лозунги, не сопоставимые с мандатом организации. За политической демагогией нередко кроется устойчивое нежелание стран Запада выполнять уставные обязательства во всей их полноте и взаимосвязи».

Среди новых аспектов злонамеренной деятельности антироссийской направленности с использованием потенциала Украины в информационном пространстве выделяется нарастающая информационная поддержка перспективных планов по возможному разделу территории Украины и поставок дальнобойных систем вооружения.

Важно выделить характерные особенности информационного пространства в пределах так называемого «украинского измерения» («український вимір»): отсутствие «цифрового» суверенитета; тотальная гегемония идеологии неонацизма; полная индифферентность органов власти всех уровней к дискриминации славянской культуры; инфантильность подавляющей части социальных групп населения Украины к действиям, направленным на последовательное уничтожение канонического православия с насаждением культа сатанизма и безбожия.

Экспресс анализ соблюдения/практического применения США и его союзниками разработанных в ООН норм и принципов ответственного поведения государств в ИКТ-среде

Решение проблемы обеспечения информационной безопасности на национальном уровне можно рассматривать только во взаимосвязи с формированием системы обеспечения международной информационной безопасности в контексте оценки поведения государств с позиций международного права.

По мнению российских и международных экспертов, практическое применение рекомендаций по нормам ответственного поведения государств в ИКТ-среде, поддержанных резолюциями 70-й, 76-й сессий Генеральной Ассамблеи ООН, может способствовать формированию системы МИБ, обеспечить снижение угрозы международному миру и стабильности.

Вместе с тем все более очевидным становится понимание ситуации, когда международные инциденты в ИКТ-среде происходят, как правило и чаще всего, вследствие злонамеренной и вредоносной деятельности специальных организаций и сил западных субъектов международного права во главе с США в когнитивном пространстве и против критически важной информационной инфраструктуры в интересах достижения политических, экономических, военных, террористических и преступных целей на глобальном и региональном уровне.

При этом Украина в настоящее время превратилась в полигон для отработки Западом социально-политических технологий с глобальными цивилизационными целями.

Информационные вбросы дезинформации, анонимные провокации, лживая пропаганда, тотальная цензура стали современными формами реализации информационной политики западными СМИ, использующих доминирующее положение в глобальном информационном пространстве.

ИИ-технологии рассматриваются как перспективное и эффективное средство борьбы за мировое господство. Западные специалисты уже используют ИИ как мощный инструмент для дезинформации и распространения языка ненависти, инспирирования конфликтных ситуаций, что не способствует поддержанию международной стабильности и безопасности.

В связи с этим в повестке обсуждаемых в ООН актуальных вопросов, влияющих на обеспечение МИБ, является проблематика использования искусственного интеллекта. Российская позиция заключается в том, что положения резолюции СБ ООН 2686 определяют необходимые базовые ориентиры (универсальные подходы), в том числе применительно к использованию технологий ИИ в контексте дезинформации и борьбы с ней.

Аспекты, представляющие угрозу неправомерного использования ИИ, предлагается обсуждаться на зарекомендовавших себя площадках, в том числе по регулированию международного сотрудничества в области безопасности ИКТ-среды.

Прошедшая в ООН в марте этого года 7-я сессия Рабочей группы открытого состава по

вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025 показала, что Запад не собирается заниматься юридическими обязательствами, а заинтересован в продвижении французского проекта Программы действий по поощрению ответственного поведения государств в сфере использования информационно-коммуникационных технологий в контексте международной безопасности.

То, что красивые слова и обещания западников отличаются от их намерений и практических действий становится все более очевидным для большинства стран. Показательным примером служит констатация факта, что в информационном пространстве сообщества западных государств завершена зачистка информационного пространства, включая контроль не только за деятельностью СМИ, но и глобальных интернет-платформ, что также противоречит нормам ответственного поведения государств в ИКТ-среде.

Некоторые направления деятельности и инструменты по обеспечению интересов Российской Федерации в информационной сфере

Основной комплекс мероприятий по защите интересов Российской Федерации в информационной сфере реализуется в рамках выполнения указов Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

В стадии завершения находится создание технической системы противодействия DDoS-атакам, которая обеспечит непрерывный мониторинг и анализ российского и зарубежного интернет-трафика с возможностью его блокирования в случае выявления вредоносности.

В целях противодействия распространению дезинформации и языка ненависти в России нашли способ рассекретить владельцев анонимных Telegram-каналов путем использования специальной нейросети.

Крупнейшими российскими IT-компаниями при поддержке государства разработан национальный Кодекс этики в сфере искусственного интеллекта, который определяет ориентиры разработчикам и пользователям для безопасного и этичного создания и применения систем с ИИ. Перспективным направлением дальнейшей реализации этого документа может являться обмен опытом с партнерами в рамках ОДКБ, ШОС и БРИКС. Российская позиция заключается в том, что ИИ рассматривается в практической плоскости, как драйвер для экономического развития в различных областях.

В Уголовный кодекс РФ предлагается внести изменения, касающиеся использования IT-технологий в качестве отягчающего обстоятельства при совершении преступлений.

В статье отражены лишь некоторые аспекты актуальной проблемы, касающейся взаимосвязи независимости и информационной безопасности России от способности государства обеспечить национальный суверенитет в информационном пространстве.

Коротков С.В., кандидат военных наук, МГТУ им. Н.Э. Баумана