Автор: admin
13.03.2022 11:20 - Обновлено 02.07.2022 16:25

Текущие негативные события и резкие изменения в военно-политической и оперативной обстановке вокруг внутреннего вооруженного конфликта на Донбассе вынудили практически перейти на круглосуточный режим работы и задействовать весь киберпотенциал НАТО и ЕС для противодействия так называемой «агрессивной вредоносной и злонамеренной политике России» в информационном пространстве.

**По оперативным расчетам для реализации скоординированных мер Североатлантического альянса и Европейского союза в рамках проведения широкомасштабной информационной войны
в настоящее время
задействованы
значительные силы общей численностью
от 150 до 200 тыс.
человек
, включая специалистов в области IT-технологий, информационно-психологических операций, компьютерной разведки, стратегической пропаганды, общественной дипломатии, взаимодействия с национальными и зарубежными СМИ, а также персонала в области обеспечения кибербезопасности.**

Основу кибервозможностей и киберпотенциала, в том числе для нанесения ущерба наиболее важным системам обеспечения жизнедеятельности государства и

населения, составляют так называемые формирования кибервойск, прежде всего США, Великобритании, Германии, Франции, Норвегии и Польши.
В настоящее время численность киберкомбатантов в этих структурах превышает несколько десятков тысяч военнослужащих и гражданского персонала.
Так,
Киберкомандование США (USCYBERCOM) – более 64 тыс.чел., киберструктуры ФРГ (Kommando Cyber und Informationsraum) и Франции – 14,5 тыс. чел. и 4 тыс. чел соответственно. Национальные кибернетические силы (NCF) Соединенного Королевства – около 2 тыс. персонала. В численности кибервойск не учтены военнослужащие специальных формирований вооруженных сил для проведения психологических операций (например, 4 Гр.ПСО Пентагона – 2,7 тыс.чел. , 77 бр ПСО Великобритании численностью 1,5 тыс. чел.).

Командные структуры кибервойск ВС государств-членов НАТО:

Бельгия – группа информационный операций (более 60 чел.);

Великобритания – управление кибернетических и информационных операций СК ВС с оперативным подчинением 77 бр ПСО 6 дивизии обеспечения СВ;

Германия – Главное командование сил кибернетических операций и информационного обеспечения, Центр информационных операций Бундесфера (более 800 чел.);

Нидерланды – командование кибернетических операций (250 чел.);

Норвегия – кибернетическое командование (1.230 чел.);

Польша – командование войск кибернетической обороны (2.000 чел.) и центр кибернетических операций (500 чел.);

Франция - кибернетическое командование ВС (4.200 чел.) и семь региональных центров кибернетических операций по 300 чел. в каждой структуре;

Чехия – командование кибернетических сил и информационных операций (500 чел.).

Вышел на полноценную боевую работу Центр кибероперациий при штабе ОВС НАТО в Европе.

Как показывает анализ эффективность деятельности этой многотысячной армии дезинформаторов, привыкших работать строго по шаблонам и указаниям, не приносит ожидаемого для «коллективного Запада» результата в информационно-психологической области. В критической и напряженной ситуации очевидна низкая компетентность и не способность обеспечить общее руководство стратегической пропагандой блока лично генеральным секретарем альянса, не говоря о его помощнике в лице начальника управления по вопросам общественной дипломатии (Public Diplomacy Division) Международного секретариата блока.

На этом поприще особой пользой не отмечена и работа Центра передового опыта НАТО в области стратегической пропаганды
(
STRATCOM COE в количестве 23 чел.), учрежденной
в
Риге
в 2014 году. Свою лепту в оправдание своего существования пытаются внести Центр передового опыта НАТО по энергетической безопасности (ENSEC COE,
г. Рига
), Центр передового опыта совместной киберзащиты НАТО (CCD COE,
г. Таллин
) и Российская информационная группа (RIG).

Поэтому в информационное пространство из расчета на обывателей вбрасываются фейки-аргументы типа «сроки российской агрессии против Украины переносятся в связи с потеплением, что затрудняет применение танков». Например, американский телеканал CNN сообщил, что российское вторжение на Украину 16 февраля не состоялось из-за погодных условий. По мнению экспертов этого информагентства, оттепель, которая установилась на границе Украины и России, не даёт замёрзнуть влажной земле, что делает её труднопроходимой для военной техники, остановившей Т-72 «Урал» и Т-90 «Владимир», несоразмерное применение силы российскими войсками (удар по роддому в Мариуполе, где занимал огневые позиции карательный батальон «Айдар»), готовность России применить химоружие и т.д.

Подобные новости делаются на основе дезинформации от спецслужб или специальных структур (формирований) для проведения информационно-психологических акций «под чужим флагом» с одной целью - отвлечь внимание мировой общественности от подготовки Украины к нападению на Донбасс вопреки Минским соглашениям.

Более пятнадцати лет подготовки американскими инструкторами киберкомбатантов из числа своих союзников по НАТО принесли определенные «положительные» результаты, которые сегодня и вылезают на поверхность как демаскирующие признаки их «зловредной деятельности».
В работе руководящими документами организации строго определено использование четырех основных способов дезинформации:

максимальное упрощение сведений и сообщений в интересах внедрения в сознание необходимых (заданных) выводов, суждений и мнений;

искажение достоверной (ценной), но не отвечающей интересам альянса, информац и и;

введение на всех уровнях тотальной цензуры с целью исключения или ограничения распространения сведений, компрометирующих или дискредитирующих деятельность НАТО;

сокрытие (замалчивание) важных сведений.

В целях обеспечения массированного применения кибервозможностей блока, максимального сосредоточения усилий на российском направлении, а также более рациональном использовании финансовых и других имеющихся ресурсов, в соответствии с последними директивными и планирующими документами альянса вся основная деятельность НАТО в информационно-коммуникационном пространстве организована и реализуется в рамках одной информационной кампании, включающей проведение нескольких стратегических информационных операций (СИО) по трем ключевым задачам (направлениям):

«создание проекции стабильности» - мероприятия СИО проводятся в информационно-коммуникационном пространстве государств-партнеров альянса с целью формирования у населения устойчивого мнения о том, что НАТО является единственной надежной военно-политической организацией, обеспечивающей безопасность в современном мире, в том числе от российской агрессии;

«сдерживание и необходимый диалог» - мероприятия СИО проводятся в информационно-коммуникационном пространстве России и ее союзников с целью предотвращения агрессии со стороны России в отношении государств – членов НАТО;

«стратегическая оборона и безопасность» - мероприятия СИО проводятся в информационно-коммуникационном пространстве государств-членов альянса с целью формирования негативного общественного мнения в западных странах к политике Российской Федерации, а также обоснования мер по расширению и укреплению блока, в том числе увеличения выделяемых финансовых затрат на его нужды.

В указанную работу усилиями США и НАТО полноценно втянут Европейский Союз. Для этого в ЕС за последние годы созданы соответствующие механизмы, сформированы пропагандистские структуры, организован процесс разработки планирующих документов на основе единых подходов к использованию информационно-коммуникационного пространства для противодействия и сдерживания России.

В этих целях с 2015 года в составе Европейской внешнеполитической службы функ ционирует
Оперативная группа стратегической пропаганды «Восток»
в тесном взаимодействии с
Европейским центром передового опыта в области противодействия «гибридным» угрозам
(
г.Хельсинки
) с бюджетом около 3 млн.евро на содержание около 80 чел., а также Центром военного планирования и управления зарубежными небоевыми миссиями ЕС (
г.Брюссель
), Агентством сетевой и информационной безопасности ЕС, Центром по обмену новостями на русском языке (
Чехия
)
.

В текущем 2022 году стратегическая пропаганда на международной арене, включая информационное обеспечение политики ЕС и политики безопасности в международных организациях и среди населения западных стран, реализуется по соответствующим скорректированным документам стратегического планирования (2015, 2016, 2018 г.г.).

Кроме мероприятий, проводимых кибервойсками и аффилированными с ними структурами, НПО и СМИ, в информационно-психологической сфере по обоснованию так называемой «злонамеренной деятельности» со стороны России, особое внимание в последние годы уделяется попыткам и наработке опыта проведения «вредон осных воздействий»
на отдельные объекты критической важной информационной инфраструктуры.

Следует отметить, что по вопросам противодействия использованию ИКТ в преступных целях в информационном пространстве нашей страны пресечено функционирование более 13 тыс. вредоносных ресурсов. В тоже время в январе и в ночь с 13 на 14 февраля т.г. США и Польша в очередной раз бездоказательно обвинили Россию в хакерских атаках на критически важные сети и правительственные ресурсы Украины. При этом газета The Washngton Post не смогла привести доказательств, что за кибернападениями стоит именно Российская Федерация. В этом контексте важно обратить внимание на заявление 14 февраля т.г. в Совете Федерации заместителя Министра иностранных дел России О. Сыромолотова о том, что «западные партнеры продолжают противодействовать реализации инициативы по разработке в рамках созданного специального комитета международной конвенции по противодействию использованию ИКТ в преступных целях».

В связи с этим важно отметить целенаправленную деятельность в политических интересах США и их союзников на международной арене и, прежде всего в ООН, по размыванию и смешению различий между вредоносным воздействием (действием) и злонамеренным воздействием (действием).

Вредоносное воздействие – любые действия вредоносных программ, приводящие к нарушению работоспособности компьютерных систем.

Примечание: Это, как правило, сфера информационно-технического воздействия на КВИО информационной инфраструктуры, обеспечивающей жизнедеятельность государства.

Злонамеренное воздействие (действие) – причинение вреда с использованием ИКТ со злым умыслом.

Примечание: Это, как правило, сфера информационно-психологического воздействия (область общественного сознания).
В этом аспекте следует рассматривать деструктивное информационно-психологическое воздействие ,
осуществляемое на политические и социально-экономические процессы,

деятельность гос.органов, а также на физических и юридических лиц в целях нанесения ущерба нац.безопасности государства. Другими целями могут быть определены, как показывает практика, ослабление обороноспособности страны, нарушение государственной и общественной безопасности, оказание содействия в принятии и заключении невыгодных законодательных актов или международных договоров, осложнение отношений с дружественными государствами, создание социально-политической напряженности, оказание влияние на избирательные компании в органы власти различных уровней, формирование угроз возникновения «ЧС», а также постепенного разрушения (девальвации) традиционных духовно-нравственных ценностей.
Основным способом
злонамеренного во
здействия
в отличие от вредоносного воздействия
(использование вредоносного ПО или софта)
является распространение дезинформации или негативного контента.
Дезинформация – распространение заведомо ложной (частично ложной или искаженной) информации с целью оказания заданного (целенаправленного) влияния на общественное мнение или политику в стране или за рубежом. Один из наиболее эффективных способов (методов) деятельности политических структур и спецслужб в различных областях с планированием и продвижением по единому замыслу ложных сведений с целью формирования неверного представления о событиях, фактах и явлениях в интересах дискредитации, компрометации или причинения прямого и косвенного ущерба субъекту воздействия и/или принятия им определенного управленческого решения.

Таким образом, смешение (умышленное) размывание различий между вредоносным воздействием (действием) и злонамеренным воздействием (действием) преследует достижение далеко идущих целей отнести к конкретной области уголовно-наказуемых преступлений в сфере высоких технологий (киберпреступлений) бездоказательную причастность неугодных государств, организаций или юридических и физических лиц к изготовлению и/или распространению негативного (деструктивного) контента (дезинформации).

В этом контексте стоит вспомнить компанию обвинений России о вмешательстве в выборную кампанию США, а потом и в ряде других западных стран. Примером, попытки завуалировать значение этих понятий представителем государственного департамента США может являться доклад Группы правительственных экспертов ООН 2015 года, в котором содержаться 11 добровольных, не имеющих силы норм ответственного поведения государств в области обеспечения международной информационной безопасности.

Проведенный краткий обзор активности в информационной сфере свидетельствует о недооценке экспертами в области IT-технологий опасности всей совокупности информационных угроз с принятием неотложных мер на международном и национальном уровнях. Вот почему руководители России и Китая посчитали важным заявить 4 февраля 2022 г. о необходимости объединить усилия международного сообщества по выработке новых норм ответственного поведения государств, в том числе юридического характера, а также универсального международно-правового документа, регулирующего деятельность государств в ИКТ-сфере. В связи с усилением и обострением противоборства в ИКТ-сфере эта задача в интересах обеспечения национальной безопасности государства должна стать одним из главных приоритетов государственной политики Российской Федерации.

Сергей Коротков, кандидат военных наук