Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ ЗАЩИТЫ ГРАЖДАН СОЮЗНОГО ГОСУДАРСТВА ОТ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ ИНФОРМАЦИИ В СОВРЕМЕННЫХ УСЛОВИЯХ ИНФОРМАЦИОННОЙ ВОЙНЫ

В.Е. МАКАРОВ

Научно-исследовательский университет «Московский институт электронной техники»

Одним из основных факторов безопасного развития Союзного государства является поддержание стабильности функционирования общественной системы. Обеспечение гражданского мира и согласия определяется как одно из важнейших условий реализации национальных интересов союзного государства во внутриполитической сфере.

Все это требует целенаправленной деятельности по нейтрализации причин и условий, способствующих возникновению конфликтов и кризисных ситуаций, которые могут вызвать нарушение единства и стабильности общественного развития, создать угрозу безопасности наших стран.

Рассматривая роль массовых коммуникаций и их влияние на политические процессы, современные политологи отмечают, что в постиндустриальном обществе власть знаний и информации становится решающей в управлении обществом, оттесняя на второй план влияние денег и государственного принуждения. Причем непосредственными носителями и, особенно, распространителями знаний и другой социально значимой информации являются средства массовой коммуникации.

Справедливо отмечается, что государственное, административное и иное силовое принуждение все больше заменяется на информационное воздействие и психологическое принуждение.

Исследователи отмечают, что иметь важную информацию значит иметь власть; уметь отличать важную информацию от неважной означает обладать еще большей властью; возможность распространять важную информацию в собственной режиссуре или умалчивать ее означает иметь двойную власть.

Хорошо известно, что наиболее опасным и эффективным средством информационно-психологического воздействия для политической системы любого субъекта международных отношений являются организационные технологии тайного внешнего информационного управления, мероприятия информационно-психологической агрессии и операции информационно-психологической войны.

Использование арсенала сил, средств и методов информационно-психологического воздействия позволяет обеспечить высокую скрытность, гибкость и многовариантность оказания политического воздействия, как в условиях мирного времени, так и в условиях политической конфронтации, чему способствуют следующие отличительные черты организации и проведения операций информационно-психологической войны:

внезапность нанесения удара по противнику;

скрытность стадии подготовки операции (в том числе – возможность скрытного, практически не выявляемого разведкой противника маневрирования силами и средствами, а также возможность их быстрого и скрытного сосредоточения вблизи границ и жизненно важных коммуникаций противника для внезапного нанесения удара);

идеальные условия для маскировки и сокрытия истинных намерений, создаваемые использованием методов психологического и информационно-технического воздействия (из средств информационно-психологической войны), возможность действовать «под чужим флагом»;

отсутствие материальных (криминалистически значимых) следов агрессии, позволяющих установить истинного агрессора и привлечь его к международной ответственности;

отсутствие необходимости физического вторжения на территорию противника и оккупации этой территории для достижения своих целей;

бездействие основного вооруженного потенциала государства, ставшего жертвой информационно-психологической агрессии, фактическое бездействие или неэффективность традиционных военно-политических союзов, созданных для отражения попыток военного вторжения и коллективной обороны от традиционных средств вооруженного нападения;

хорошие возможности для нанесения жертве агрессии (в условиях мирного сосуществования) ущерба, сравнимого с результатами военных действий на его территории, без официального объявления войны или каких-либо иных изменений дипломатических отношений;

серьезные трудности, испытываемые жертвой агрессии при обнаружении источника информационной (психологической) агрессии, ее квалификации и определении степени опасности и агрессивности выявленных атак (нападений) на его информационные ресурсы и социальную сферу информационно-психологических отношений, а также истинных масштабов и целей агрессии. Следует также отметить, что, в силу латентности протекания организационной и активной стадии информационно-психологической операции жертва агрессии может обнаружить, что на нее напали, только на завершающей стадии проведения такой операции, когда локализация ущерба уже вряд ли возможна;

трудности, испытываемые жертвой агрессии при выборе системы мер реагирования на информационно-психологическую агрессию, предотвращения нанесения этим нападением ущерба государственным интересам и выборе адекватного ответа (ударом на удар).

отсутствие военно-политических блоков, союзов и коалиций, призванных обеспечивать коллективную безопасность от внешней агрессии в информационно-психологической сфере, что составляет жертву информационно-психологической агрессии один на один с агрессором без какой-либо заранее подготовленной поддержки извне.

Важную роль использования организационных форм и технологий информационно-психологического воздействия в качестве инструмента внешней политики подтверждают положения активно разрабатываемой в США концепции «информационного сдерживания» – управления кризисными ситуациями с помощью превентивных акций по информационно-психологическому воздействию на население и властные структуры в зонах возможного возникновения конфликтов

Напомним, что термин информационная война во многом навеян взглядами древнекитайского философа Сунь-Цзы, который в своем трактате «Искусство войны» первым обобщил опыт информационного воздействия на противника:

«Во всякой войне, как правило, наилучшая политика сводится к захвату государства целостным; разрушить его значительно легче. Взять в плен армию противника лучше, чем ее уничтожить… Одержать сотню побед в сражениях – это не предел искусства. Покорить противника без сражения – вот венец искусства».

Сунь-Цзы имел в виду информационную операцию*: «Разлагайте все хорошее, что имеется в стране противника. Разжигайте ссоры и столкновения среди граждан вражеской страны»*.

С конца прошлого века объектом информационной войны стали кибернетические системы. Параллельно развернулись информационная война за человеческие умы. Правительственные структуры, средства массовой информации и неформальные движения включились в информационно-психологические операции с целью управления общественным мнением. Деструктивные культы и террористические организации умудрились даже делать «большие деньги» на своих адептах и смертниках. Невиданной эффективности достигли политтехнологи, составившие угрозу информационно-психологических пространствах социумов.

Обобщая вышеизложенное, в интересах обеспечения комплексной защиты граждан союзного государства от деструктивного воздействия информации в современных условиях информационной войны, представляется целесообразным создать специальную систему информационного противодействия по организации и ведению информационного противоборства, а также координации осуществления на практике структурными подразделениями министерств и ведомств, органов управления союзного государства на уровне регионов, оборонительных и наступательных информационных операций.

Каковы могут быть основные функции такой системы?

Прежде всего, выявление и прогнозирование угроз в информационной сфере, и проведение комплекса тактических, оперативных и стратегических мероприятий по их предупреждению и нейтрализации.

Следующий момент – создание и поддержание в готовности сил и средств информационного противодействия, а также эффективное управление ими.

Для того, чтобы объединить весь комплекс мероприятий в единое целое, необходимо интегрировать их в рамках организационно-аналитической системы. Она может представлять собой систему управления проведением мероприятий различных уровней союзного государства: общефедерального, регионального, муниципального, профессионального, группового и индивидуального.

Система организации действий сможет обеспечить:

участие в решении проблемы специалистов всех необходимых профилей (политологов, социологов, психологов, психоаналитиков, криминалистов, специалистов информационного противоборства, журналистов и т.д.)

всестороннюю и своевременную обеспеченность проведения всего комплекса необходимых мероприятий, а также планирование и управление ими на основе современных методов работы (сетевое планирование, целевое программное управление, стратегическое управление и т.д.).

Знание целей, задач, методов и средств осуществления информационно-психологических операций в современной информационной войне позволяет определить необходимые и эффективные меры по противодействию информационно-психологическим мероприятиям вероятного противника, направленным на подрыв морально-психологического состояния, дезинформацию и деморализацию индивидов, социальных групп, общества и личного состава силовых структур, дезорганизацию деятельности силовых структур.

Эффективность работы по противодействию информационно-психологических операций и психологическим диверсиям вероятного противника будет в решающей степени зависеть от того, насколько удастся на практике реализовать принципы упреждения, доходчивости и эмоциональной насыщенности проводимых мероприятий.

То есть результаты противодействия будут определяться тем, в какой мере специалисты и психологи учтут закономерности функционирования социальной психики в современной социально-политической обстановке.

Защита личности, социальных групп, социальных систем и всего социума от информационно-психологических операций вероятного противника представляет собой систему мероприятий по: прогнозированию, профилактике, оценке, срыву информационно-психологического воздействия противника на наши войска и население; ликвидации его негативных последствий.

Прогнозирование информационно-психологических операций вероятного противника заключается в превентивной оценке специалистами в области информационной борьбы, руководителями силовых структур, общественными организациями, штабами, органами воспитательной работы сил и средств подрывных акций, которыми может располагать реальный или потенциальный противник.

Важным моментом прогнозирования является определение каналов информационно-психологического воздействия на социум и личный состав силовых структур. Руководители государственных структур, специалисты в области информационной борьбы, руководители общественных организаций, гражданского общества, в том числе СМИ должны выделить потенциальные объекты наиболее интенсивного информационно-психологического воздействия вероятного противника.

Как показывает практика, специалисты подрывных акций подходят дифференцированно к аудиториям, на которые осуществляется их влияние.

Важным моментом прогнозирования является определение возможной тематики и символики информационно-психологических операций противника с целью упреждения, снижения их эффективности или нейтрализации.

Оценка осуществляющейся противником информационно-психологической акции заключается в выявлении ее истинных целей и объектов. Планируя такие акции, специалисты информационно-психологических операций будут нацеливать ее на дезинформацию, запугивание, изменение настроений, системы отношений, желаний, активности, схем поведения наших граждан. Как показывает опыт, важнейшей задачей информационно-психологических операций выступает дезинформация противника.

Можно отметить, что в системе регулирования социальных и политических отношений в современном информационном обществе центральное место занимает государственная информационная политика – деятельность системы органов государственной власти и управления в информационно-психологической сфере, компетенция которых определяется действующим, стремительно развивающимся информационным законодательством.

В сложных современных условиях государственная информационная политика во многом способствует формированию и развитию новой системы информационно-психологических отношений, позволяющих современному обществу перейти на новый, революционный, этап развития, обеспечивает защиту национальных интересов и информационно-психологическую безопасность личности, общества и государства в изменяющихся условиях.

Между тем, сегодня государственная информационная политика сама находится в стадии формирования, поиска и испытания новых методов, способов и технологий государственного управления, эффективных в условиях информационного общества.

Для информационной политики важное значение имеет рассмотрение информационного пространства как пространства не столько физического, сколько социального типа.

Важной отличительной особенностью информационного пространства, которая позволяет рассматривать его именно с такой точки зрения, является то, что в отличие от других пространств, где физическую географию определяет власть, в информационном пространстве задают структуру власти информация и знания.

Значимость в информационном пространстве для информационной политики имеют те его компоненты и процессы, воздействие на которые средствами и методами информационной политики позволяет влиять на перспективы, на конкретные лица, которые принимают решения, контролировать системы сбора, обработки, хранения и передачи информации, преумножать ресурсы

Государственная информационная политика по обеспечению информационной безопасности Союзного государства в условиях информационно-психологической войны является составной частью государственной политики по обеспечению национальной безопасности в части, касающейся деятельности системы органов государственной власти по достижению национальных интересов страны и обеспечению информационно-психологической безопасности личности, общества и государства в условиях непосредственной угрозы развязывания государствами-участниками информационного противоборства крупномасштабной информационно-психологической агрессии (информационно-психологической войны) в отношении Союзного государства.

Список литературы

1. В.Е. Политические и социальные аспекты информационной безопасности: монография. – Таганрог: издатель С.А. Ступин, 2015. – 352

2. Брусницин Н.А.Информационная война и безопасность – М.: Вита-Пресс, 2001. – 280 с.

3. Манойло А.В. Государственная информационная политика в особых условиях: монография. М.: МИФИ, 2003. – 218 с.

4. Панарин И.Н. Информационная война и коммуникации. – М.: Горячая линия – Телеком, 2014. – 236 с.

5. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ DLP-СИСТЕМЫ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

В.В. МАЛИКОВ, М.А. БАБИЧ, А.В. МАКАТЕРЧИК

Белорусский государственный университет информатики и радиоэлектроники

В настоящее время, как правило, главными экономическими активами компаний и государств являются объекты интеллектуальной собственности, полученные в результате интеллектуальной деятельности с затратой значительных материальных и финансовых ресурсов. Несанкционированный доступ к таким активам приводит к их краже, что негативно влияет на экономику стран и приводит к банкротству компаний.

Обеспечение защиты от утечки конфиденциальной информации является сложной и многоуровневой задачей, которая включает в себя разграничение уровней досту-