"ПРАВО ЗНАТЬ: история, теория, практика"
N 7–8 (43–44) июль-август 2000 г.

ПРИНЦИПЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕРМИНОЛОГИЯ

Значение терминов, используемых в настоящих "Принципах":

1. Информационная сфера – область деятельности, относящейся к созданию, передаче и использованию информации, включая личное и общественное сознание, информационную и телекоммуникационную инфрастуктуру и собственно информацию.

2. Информационные ресурсы – информационная инфраструктура (аппаратура и системы создания, обработки, хранения и передачи информации), включая файлы и базы данных и собственно информацию и информационные потоки.

3. Информационная война – конфронтация между государствами в информационной сфере, направленная на нанесение ущерба информационным системам, процессам и ресурсам и жизненно важным структурам, нарушение работы политических, экономических и социальных систем, а также массовое психологическое манипулирование населением с целью дестабилизации общества и государства.

4. Информационное оружие – методы и средства, используемые для нанесения ущерба информационным системам, процессам и ресурсам, оказания отрицательного информационного воздействия на оборонные, административные, политические, социальные, экономические и иные жизненно важные структуры государства, а также массовое психологическое манипулирование населением с целью дестабилизации общества и государства.

5. Информационная безопасность – защита основных интересов личности, общества и государства в сфере информации, включая информационную и телекоммуникационную инфрастуктуру и собственно информацию и ее параметры, такие, как полнота, объективность, доступность и конфиденциальность.

6. Угроза информационной безопасности – факторы, угрожающие интересам личности, общества и государства в сфере информации.

7. Международная информационная безопасность – состояние международных отношений, препятствующее нарушению международной стабильности и возникновению угрозы безопасности государств и международного сообщества в сфере информации.

8. Незаконное использование информационных и телекоммуникационных систем и информационных ресурсов – использование информационных и телекоммуникационных систем и информационных ресурсов без соответствующего разрешения или в нарушение установленных правил, законодательства или принципов международного права.

9. Несанкционированное вмешательство в информационные и телекоммуникационные системы и информационные ресурсы –вмешательство– в процесс сбора, обработки, накапливания, хранения, представления, поиска, распространения и использования информации с целью нарушения нормальной работы информационных систем или полноты, конфиденциальности и доступности информационных ресурсов.

10. Жизненно важные структуры – государственные системы, структуры и институты, умышленное вмешательство в информационные ресурсы которых может напрямую сказаться на национальной безопасности (транспорт, энергетика, кредитование и финансы, связь, государственные административные структуры, оборонное ведомство, силовые органы, стратегические информационные ресурсы, научно–исследовательские организации и научно–технические разработки, установки повышенной технологической и экологической опасности, органы борьбы с чрезвычайными ситуациями).

11. Международный информационный терроризм – использование телекоммуникаций и информационных систем и ресурсов или воздействие на такие системы и ресурсы в международной информационной сфере с целью совершения террористических актов.

12. Международная информационная преступность – использование телекоммуникаций и информационных систем и ресурсов или воздействие на такие системы и ресурсы в международной информационной сфере в противозаконных целях.

ПРИНЦИП I

1. Деятельность государств и иных субъектов международного права в международной информационной сфере должна способствовать всеобщему социальному и экономическому развитию и осуществляться в соответствии с задачами сохранения глобальной стабильности и безопасности, соблюдения суверенитета других государств, интересов безопасности, принципов мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, соблюдения прав и свобод человека.

2. Такая деятельность должна также осуществляться в соответствии с правом каждого человека запрашивать, получать и распространять информацию и взгляды, гарантированным соответствующими документами ООН, с учетом того, что это право может быть ограничено в законодательном порядке с целью защиты интересов безопасности государства.

3. В то же время, любые государства и иные субъекты международного права должны иметь равные права на защиту своих информационных ресурсов и жизненно важных структур от незаконного использования или несанкционированного информационного вмешательства, и могут рассчитывать на поддержку мирового сообщества при реализации этих прав.

ПРИНЦИП II

Государства будут стремиться сдерживать угрозы в сфере международной информационной безопасности, и будут с этой целью воздерживаться от:

• разработки, создания и применения средств воздействия или нанесения ущерба информационным ресурсам и системам другого государства;

• намеренного использования информации для воздействия на жизненно важные структуры другого государства;

• использования информации для подрыва политических, экономических и социальных систем другого государства, психологического манипулирования населением с целью дестабилизации общества;

• несанкционированного вмешательства в информационные и телекоммуникационные системы и информационные ресурсы, а также незаконного использования таких систем и ресурсов;

• попыток доминирования и контроля в сфере информации;

• запрещения доступа к новейшим информационным технологиям и создания ситуации, в которой другие государства попадают в противоречащую их интересам технологическую зависимость в сфере информатизации;

• поддержки деятельности международных террористических, экстремистских и преступных организаций, групп или отдельных правонарушителей, которая представляет угрозу информационным ресурсам или жизненно важным структурам какого–либо государства;

• составления и принятия планов и доктрин, предусматривающих возможность развязывания информационных войн и способных спровоцировать гонку вооружений и вызвать напряженность в отношениях между государствами, а также собственно ведения информационных войн;

• использования информационных технологий и средств во вред правам и свободам человека в области информации;

• распространение информации через государственные границы в нарушение принципов международного права или законодательства отдельных государств;

• манипулирование информационными потоками, дезинформация и утайка информации в целях подрыва психологической и духовной обстановки в обществе, разрушения традиционных культурных, моральных, этических и эстетических ценностей;

• информационная экспансия и установление монополии на информационные и телекоммуникационные инфраструктуры другого государства, включая условия их функционирования в международной информационной сфере.

ПРИНЦИП III

Организация Объединенных Наций и соответствующие структуры в системе ООН будут способствовать международному сотрудничеству, направленному на сдерживание угроз в сфере международной информационной безопасности и создание с этой целью международной законодательной базы для:

• определения характеристик и создания классификации информационных войн;

• определения характеристик и создание классификации информационного оружия, а также методов и средств, которые могут рассматриваться как информационное оружие;

• ограничения торговли информационным оружием;

• запрещения разработки, распространения и применения информационного оружия;

• предотвращения угрозы информационных войн;

• приравнивания угрозы применения информационного оружия против жизненно важных структур к угрозе применения оружия массового поражения;

• создания условий для равного и безопасного международного информационного

обмена на основе общепризнанных правил и принципов международного права;

• предотвращения использования информационных технологий и средств в террористических и иных преступных целях;

• предотвращения использования информационных технологий и средств для воздействия на общественное сознание в целях дестабилизации общества и государства;

• разработки процедуры взаимного оповещения и предотвращения несанкционированного использования информации для воздействия на другие государства;

• создания международной системы мониторинга для отслеживания угроз в сфере информации;

• создания механизма мониторинга соблюдения условий режима международной информационной безопасности;

• создания механизма урегулирования конфликтных ситуаций в сфере информационной безопасности;

• создания международной системы сертификации информации и телекоммуникационных технологий и средств (включая технику и программное обеспечение) с целью гарантии их информационной безопасности;

• создания системы международного сотрудничества между силовыми органами с целью предотвращения и борьбы с преступлениями в информационной сфере;

• добровольного приведения национальных законодательств в соответствие с необходимостью обеспечения информационной безопасности.

ПРИНЦИП IV

Государства и иные субъекты международного права должны нести международную ответственность за деятельность в информационной сфере, осуществляемую ими или под их юрисдикцией или под эгидой международных организаций, членами которых они являются, а также за соответствие этой деятельности принципам, изложенным в настоящем документе.

ПРИНЦИП V

Любой спор между государствами и иными субъектами международного права, возникший в связи с применением настоящих принципов, будет урегулирован на основании установленных процедур мирного урегулирования споров.