Сарычев Н.В., Мельниченко Д.В.

Внешние и внутренние угрозы информационной безопасности России

Информационная безопасность – защищенность информационной среды личности, общества и государства от преднамеренных и непреднамеренных угроз и воздействий. Обеспечение информационной безопасности Российской Федерации тесно взаимосвязано с решением внутренних проблем страны: проблем обеспечения политической, экономической, военной, социальной и других видов национальной безопасности. Для обеспечения внешнего аспекта информационной безопасности большая роль должна отводиться взаимодействию с информационными органами других стран.

Ключевые слова: *противодействие идеологии терроризма, информационная сфера, информационные угрозы, информационная безопасность, защита от информационно-психологических угроз.*

Информационная сфера России характеризуется активным развитием современных средств информационного обмена и различного типа компьютерных систем. Это создает условия для обеспечения информационной поддержки деятельности аппарата управления на всех уровнях и во всех ветвях власти.

Вместе с тем слабое внимание, уделяемое проблемам обеспечения информационной безопасности, создает объективные условия для незаконного доступа к закрытой информации, ее хищения или разрушения. Особую опасность имеет возможность манипуляций различного рода информацией для негативного воздействия на процесс принятия политических решений [1].

В перечне видов угроз информационной безопасности, обозначенных в Доктрине [2], стоит обратить особое внимание на:

- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Основными целями защиты от информационно-психологических угроз для России являются:

1) защита от разрушительных информационно-психологических воздействий среды общества, психики населения, социальных групп граждан;
2) противодействие попыткам манипулирования процессами восприятия информации населением со стороны враждебных России политических сил, проводимых е целью ослабления обороноспособности государства;
3) отстаивание национальных интересов, целей и ценностей России в информационном пространстве (глобальном, национальном, региональном, субрегиональном, стран СНГ);

4) постоянное отслеживание отношений российское общества к важнейшим проблемам национальной безопасности (диагностика общественного мнения, психологического состояния нации).

Ведущие страны мира в настоящее время располагают мощным потенциалом информационного противоборства (прежде всего, США, Китай, Израиль, Франция, Великобритания, Германия), который может обеспечить им достижение политических и экономических целей, тем более что отсутствуют международные юридические нормы ведения информационной борьбы.

В Доктрине информационной безопасности Российской Федерации определены следующие основные источники внутренних угроз информационной безопасности [2].

К внутренним источникам относятся:

– критическое состояние отечественных отраслей промышленности;
– неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
– недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
– недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
– неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
– недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
– недостаточная экономическая мощь государства;
– снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
– недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
– отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления,

кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

- нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;
- недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;
- распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;
- деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.
- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;
- распространение за рубежом дезинформации о внешней политике Российской Федерации;
- нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;
- попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях [2].

На основе национальных интересов РФ в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов РФ в информационной сфере.

Первая составляющая национальных интересов РФ в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов РФ в информационной сфере включает в себя информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов РФ в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертая составляющая национальных интересов РФ в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России [3].

По мнению А.Ю. Кирьянова [1], основными задачами по реализации и защите национальных интересов на современном этапе развития России в информационной сфере являются следующие.

1. Разработка и принятие долгосрочной программы по обеспечению выхода на уровень ведущих стран мира в области создания систем информатики и управления, основанных на новейших информационных технологиях.
2. Обеспечение свободы получения и распространения информации гражданами, другими субъектами общественных отношений в интересах формирования гражданского общества, демократического правового государства, развития науки и культуры.
3. Обеспечение надежной защиты информационного потенциала России (т.е. совокупности информации, обеспечивающей национальные интересы страны; систем ее получения, хранения, переработки и распространения; его субъектов) от неправомерного его использования в ущерб охраняемым

законом интересам личности, общества и государства. Осуществление контроля за экспортом из страны интеллектуальной продукции, а также информационных банков данных. Организация эффективной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности.

4. Развитие взаимодействия государственных и негосударственных систем информационного обеспечения в целях более эффективного использования информационных ресурсов страны.
5. Совершенствование системы нормативно-правовых актов, регулирующих отношения собственности и соблюдения баланса интересов личности, общества и государства в сфере формирования, хранения и использования информационных ресурсов. Формирование и развитие федеральных и региональных центров сертификации систем информационной защиты и их элементов.
6. Противодействие целенаправленным действиям по дезинформированию органов власти, населения страны, использованию каналов информационного обмена для нарушения систем управления различными сферами жизнедеятельности государства.
7. Создание общего информационного пространства стран СНГ в интересах содействия интеграционным процессам, повышения эффективности взаимодействия в реализации общих интересов. Включение России в международную систему информационного обмена с учетом обеспечения российских национальных интересов и противодействия акциями информационной интервенции.
8. Обеспечение на международном уровне принятия решений о безусловном запрете на использование информационного оружия в мирное время.

Далее предлагается сосредоточить внимание на роли государства в области защиты информации. Общие положения по защите информации устанавливает Федеральный закон «Об информации» (ст. 16). Закон рассматривает защиту информации как комплекс «правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2) соблюдение конфиденциальности информации ограниченного доступа;
3) реализацию права на доступ к информации».

Последняя цель, на первый взгляд, не имеет отношения к защите информации. На это не так. Защищать необходимо не только информацию ограниченного доступа, но и открытую информацию, доступ к которой должен быть неограничен. Это также задача государства в отношении информации, предоставляемой для

всеобщего сведения органами государственной власти и органами местного самоуправления.

Следующая категория защищаемой информации – эта информация ограниченного доступа, находящаяся в любом режиме конфиденциальности. Но роль государства принципиально различна в обеспечении различных режимов.

Общедоступную информацию следует защищать от блокирования доступа, уничтожения, модификации (искажения). Информацию ограниченного доступа – от уничтожения, модификации, незаконного копирования, разглашения, незаконного доступа, незаконного использования [4].

Учитывая глобальный характер процессов информатизации и появление международной киберпреступности, мировое сообщество должно иметь межгосударственные организационные структуры но координации работ в области информационной безопасности.

Основным международным органом является Организация Объединенных Наций и созданный ею Совет Безопасности. Эти органы координируют усилия государств по осуществлению мероприятий в области обеспечения информационной безопасности и борьбы с преступлениями в сфере информационных технологий. Спорные вопросы на межгосударственном уровне решает Международный суд.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти федерального уровня, уровня субъектов Российской Федерации, ведомственных структур, а также служб предприятий и организаций.

Итак, в связи с новейшими научно-техническими достижениями в области информатики и информационных технологий современное соперничество государств и других объектов социальной природы характеризуется появлением нового фактора – информационного. Через целевое воздействие на информационную среду реализуются угрозы национальной безопасности в различных сферах человеческой деятельности. В политической сфере все большую значимость приобретает информационно-психологическое воздействие с целью формирования отношений в обществе, его реакции на происходящие процессы. В экономической сфере растет уязвимость экономических структур от недостоверности, запаздывания и незаконного использования экономической информации. В военной сфере исход вооруженной борьбы все в большей степени зависит от качества добываемой информации и уровня развития информационных технологий, на которых основываются системы разведки, радиоэлектронной борьбы, управления войсками и высокоточным оружием. В сфере духовной жизни возникает опасность развития в обществе с помощью электронных средств массовой информации агрессивной потребительской идеологии, распространения идей насилия и нетерпимости и других негативных воздействий на сознание и психику человека. Информационная среда, являясь системообразующим фактором во всех видах национальной безопасности (политической, экономической, военной, и др.), в то же время представляет собой самостоятельный объект защиты.

Литература

1. Кирьянов А.Ю. Сущность информационного аспекта национальной безопасности Российской Федерации // Международное публичное и частное право. – 2005. – № 3. – С. 42.
2. Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000. № Пр. 1895 // Российская газета. – 2000. – № 187.
3. Ковалева Н.Н. Информационное право России: учебное пособие. – М.: здательско-торговая корпорация «Дашков и К», 2007. – 234 с.
4. Волчинская Е.К. Роль государства в обеспечении информационной безопасности // Информационное право. – 2008. – № 4. – С. 9–16.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие. – СПб.: Питер, 2008. – С. 86–87.