Тема 7: Информационная безопасность.

Важнейшими задачами обеспечения информационной безопасности Российской Федерации являются:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

[Концепция национальной безопасности РФ в редакции Указа Президента РФ от 10.01.2000 г. №24]

Проблема создания глобального информационного общества, в котором была бы прочно гарантирована информационная безопасность, стала одной из важнейших составляющих международных отношений XXI века, предметом тщательного рассмотрения многих мировых форумов, включая “большую восьмерку”. Все больше международных экспертов выделяют в списке наиболее важных угроз человечеству в XXI веке угрозу информационной безопасности и признают, что она встала в один ряд с проблемами экологии, энергетики и пр.

К концу XX века стремительное развитие и повсеместное внедрение новых информационных и телекоммуникационных технологий стало новым этапом экономического и научно-технического прогресса человеческой цивилизации и необходимым условием дальнейшего развития общества. Современная трансформация российского общества характеризуется возрастающей ролью информационной сферы, “представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений”.

Общепризнанно, что индустрия информатизации, телекоммуникации и связи, информационных услуг на современном этапе развития цивилизации является одной из наиболее динамично развивающихся сфер мировой экономики, способной конкурировать по доходности с топливно-энергетическим комплексом, автомобилестроением, производством сельскохозяйственной продукции и определяющей наукоемкость промышленной продукции, ее конкурентоспособность на мировом рынке.

В то же время необходимо отметить, что информационная инфраструктура, информационные ресурсы во все большей степени становятся ареной межгосударственного соперничества за мировое лидерство, достижение конкурирующими сторонами определенных стратегических и тактических политических целей. Индивидуальное, групповое и массовое сознание людей все в большей степени зависят от деятельности средств массовой информации и массовой коммуникации. Вошли в обиход, в том числе и в международных

отношениях, такие понятия, как “информационная война”, “информационное противодействие”, “информационная операция” и т. п.

Во-первых, существенно возросла значимость информации в важнейших областях общественной жизни, что во многом определяет перспективы успешного осуществления социально-политических и экономических преобразований, в том числе и в России. К началу XXI века наиболее развитые страны вплотную подошли к новому этапу развития, получившего название “информационное общество”.

Во-вторых, информация прочно вошла в перечень властных ресурсов современного государства. Функционирование системы власти и властных отношений сегодня не возможны без информации и средств ее сбора, обработки, хранения и распространения.

В-третьих, наблюдается расширение функций информации. Если раньше информация во внешней политике использовалась в основном для освещения международной деятельности или ее сокрытия (дезинформация), то сегодня многие политические цели могут достигаться путем информационного воздействия на правящую элиту, армию, население, общество в целом. Решающая роль информации принадлежит в формировании общественного мнения о внешнеполитической деятельности государства.

В-четвертых, появляются новые черты в характере современного глобального информационного противоборства. Развитие средств и систем воздействия на информационное пространство других государств ставит проблему разработки теоретических и практических основ ведения информационной борьбы. Позиция Российской Федерации заключается в закреплении обязательств неконфронтационного характера развития информационных отношений в системе международного права. Предлагаемые Россией политические резолюции по информационной проблематике неизменно получают все большее одобрение в ходе голосования на Генеральной Ассамблее ООН.

[Будейкина Надежда Александровна. «Информационная безопасность России и современные международные отношения» 20.10.2003 19:42 | В.С.Денисенко Научный руководитель: к. и. н., доц., Оберемко Т.В.]

“Сегодня расстановка сил в мире изменилась. Мы движемся к совершенно другой структуре сил, разделяющей мир не на две, а на три четко определенные противоположные враждующие цивилизации. Символ Первой, как и прежде, - мотыга, Второй - конвейер, а Третьей - КОМПЬЮТЕР.

В разделенном на трое мире сектор Первой Волны поддерживает сельскохозяйственные и минеральные ресурсы, сектор Второй Волны обеспечивает дешевый труд и производит массовую продукцию, а быстро растущий сектор Третьей Волны использует НОВЫЙ СПОСОБ ДОМИНИРОВАНИЯ - СОЗДАНИЕ И ЭКСПЛУТАЦИЮ ЗНАНИЙ.

Народы цивилизации Третьей Волны продают ИНФОРМАЦИЮ и НОВОВВЕДЕНИЯ, менеджмент, культуру и поп-культуру, новые технологии,

программное обеспечение, образование, педгогику, медицинские, финансовые и другие услуги всему миру".

Поэтому у России, как самой образованной стране в мире, есть шанс для процветания. Необходимо только серьезно подойти к проблеме информационной безопасности.

Следует отметить, что проблема обеспечения информационной безопасности в нашей стране длительное время не только не выдвигалась, но и фактически игнорировалась. При этом считалось, что путем тотальной секретности и различными ограничениями можно обеспечить информационную безопасность страны.

Только сейчас Российское государство начинает серьезно и ответственно подходить к проблеме определения и отстаивания жизненно важных интересов, реальных и потенциальных угроз в информационной сфере. Российская политическая элита начинает осознавать необходимость решения проблем обеспечения информационной безопасности.

Вот несколько цитат из доклада министра Российской Федерации по связи и информатизации Л.Д.Реймана, которые характеризуют процесс создания глобального информационного пространства. (семинар "Глобализация информационного пространства: вызовы и новые возможности для России" прошел 13 апреля 2000 года в Центре стратегических разработок).

"Конец 20 века ознаменовался огромным прогрессом в развитии телекоммуникационных технологий. Сегодня, тридцать лет спустя после создания первых компьютерных сетей и восемь лет спустя после того, как ИНТЕРНЕТ приобрел современные очертания, говорить о глобальном информационном пространстве стало не только теоретически интересно, но и практически необходимо. Я приведу простой пример.

Пятьдесят лет тому назад, если вы хотели переслать 30 страниц текста на расстояние 5 тысяч километров, то вам потребовалось бы примерно десять дней и стоило бы это около 30 долларов за услуги почтовой связи.

Двадцать лет тому назад вы бы, наверное, прибегли к услугам факса. Это заняло бы у вас примерно час, и стоимость составляла где-нибудь 50 долларов.

Сегодня, если говорить о самых лучших сетях передачи данных, на это требуется не более 3 СЕКУНД и стоимость составит около 3 центов.

Таким образом, стоимость упала в тысячу раз, скорость возросла в 300 тысяч раз. *Колоссальное увеличение скорости при одновременном снижении стоимости, появление практической возможности передачи мультимедийной информации в реальное время, увеличение скорости систем поиска и обработки информации в МИЛЛИОН РАЗ - это основы будущего развития всех сфер жизни общества".*

Вывод ведущего китайского теоретика информационной войны Шэнь Вэй гуана, который он сформулировал в своей книге "О новой войне": "Чтобы защитить политическую безопасность страны, нужно НАУЧИТЬСЯ ВЕСТИ ИНФОРМАЦИОННУЮ ВОЙНУ с использованием различных средств массовой информации".

Однако по объективным и субъективным причинам, принятие разработанной Доктрины информационной безопасности Российской Федерации затянулось. (Она была утверждена уже новым Президентом Российской

Федерации Владимиром Путиным лишь 9 сентября 2000 года), как официально принятая система взглядов на проблему обеспечения информационной безопасности, методы и средства защиты жизненно важных интересов личности, общества, государства в информационной сфере.

НЕКОТОРЫЕ ТЕЗИСЫ ДОКТРИНЫ.

Доктрина служит основой для:

-формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

-подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

-разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

1.Первая составляющая национальных интересов Российской Федерации 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.

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

3.Третья составляющая национальных интересов Российской Федерации 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.

4.Четвертая составляющая национальных интересов Российской Федерации 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.

Угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

1.Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.
2.Угрозы информационному обеспечению государственной политики Российской Федерации.
3. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.
4.Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относятся:
1).деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
2).стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
3).обострение международной конкуренции за обладание информационными технологиями и ресурсами;
4).деятельность международных террористических организаций;
5).увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
6).деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
7).разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:
1).критическое состояние отечественных отраслей промышленности;
2).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,
3).снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
4).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;

5).недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
6). неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
7).недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
8) недостаточная экономическая мощь государства;
9).снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
10).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;
11).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.

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

1.К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

2.Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

3.Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:
- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Основными мероприятиями по обеспечению информационной безопасности Российской Федерации в сфере внешней политики являются:
1.разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;
2.разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;
3.создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;
4.совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;
5.совершенствование информационного обеспечения субъектов Российской Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

Основными направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются:
*развитие в России основ гражданского общества;
*создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;
*выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, *воспитанием патриотизма* и гражданской ответственности за ее судьбу;
*совершенствование законодательства Российской Федерации, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;
*государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей Российской Федерации;
*формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;
*разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности федеральных органов государственной власти и общественных объединений,

обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;
*разработка специальных правовых и организационных механизмов *недопущения противоправных информационно-психологических воздействий на массовое сознание общества*, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей Российской Федерации, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;
**введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение*;
*противодействие *негативному влиянию иностранных религиозных организаций и миссионеров*.

Информационная безопасность - это состояние защищенности информационной среды общества и политической элиты, обеспечивающее ее формирование и развитие в интересах политической элиты, граждан и государства.

Информационная среда общества - это совокупность информационных ресурсов, система формирования, хранения, распространения, использования и защиты информации, информационной инфраструктуры.

Угроза информационной безопасности - фактор или совокупность факторов, создающих опасность функционированию и развитию информационной среды общества.

Сегодня правомерно утверждать: чем большими информационными возможностями обладает государство, тем вероятнее (при прочих равных условиях) оно добивается стратегических геополитических преимуществ. В этом контексте становится понятной оценка военно-политическим руководством США и Китая информации как стратегического ресурса и объяснимы причины постоянного увеличения ассигнований на развитие и совершенствование информационных технологий.

Итак, каковы же главные тенденции геополитического развития мира в 21 веке?

1. Происходит быстрое формирование глобального всепланетарного общества, на основе развертывания информационной и телекоммуникационной революции.
2. Растут масштабы кризиса всей духовной сферы жизнедеятельности человечества (рост наркомании, преступности и т.д.).
3. В мире создано единое глобальное информационное пространство всей планеты, в котором развернулось геостратегическое информационное противоборство между ведущими странами мира за достижение превосходства в мировом информационном пространстве.
4.Таким образом, нужно сделать вывод о том, что национальная безопасность России в 21 веке, в основном, будет зависеть от эффективного функционирования информационной среды общества (т.е. способности психики политической элиты и населения России получать, обрабатывать, передавать, хранить и защищать информацию).

[Игорь Николаевич Панарин — политолог, профессор Дипломатической Академии МИД России, кандидат психологических наук, доктор политических наук, академик Академии Военных Наук. Член Научно-Методического Совета при Центральной избирательной комиссии Российской Федерации, член Экспертного Совета Комитета по СНГ Совета Федерации.
Информационная безопасность]

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ КАК РЕШАЮЩИЙ ФАКТОР В СТРАТЕГИИ ВЫЖИВАНИЯ ЧЕЛОВЕЧЕСТВА

Разработка парадигм выживания человечества стала сегодня важнейшей проблемой большинства областей научного знания и техники. Этими вопросами занимаются в равной степени и философия, и медицина, и экология, и информатика, и биология, и социология, и ноосферология и т.д.. в концепции устойчивого развития страны, человека, общества в целом должны быть включены прежде всего те механизмы и те средства, которые непосредственно работают на защиту индивида, на охрану его прав и личных интересов, его здоровья и свободы. В контексте этих проблем особенно следует выделить вопросы обеспечения информационной безопасности личности, которая играет нынче важнейшую роль в стратегии выживания человечества

Информационная безопасность личности характеризуется защищенностью психики, сознания от опасных информационных воздействий (манипулирования, дезинформирования и т.п.). Она зависит как от личностных качеств индивида, так и от моральных, социальных и правовых условий в обществе Homo Sapiens отличается от животных, прежде всего сознанием, разумом. Мозг человека, его нервная система - это информационная система, функциональные возможности которой по получению, запоминанию, обработке, передаче и использованию информации значительно превосходят возможности животных. Но и уязвимость этой системы выше. Ясно, например, что посредством целенаправленного информационного воздействия практически невозможно подвести к самоубийству животное или ребенка. Подростка же или взрослого человека - не так уж сложно.

Известно, что непременными условиями манипулирования человеком, группой людей является неинформированностъ или дезинформированность, отсталость личности и общества в области овладения современными средствами массовой информации или изолированность от них. Современные процессы в мире и в наших странах подтверждают это весьма наглядно. Одной из существенных информационных опасностей является распространение "электронного контроля" за жизнью, настроениями, планами граждан, политических организаций и т.д. Уже появляются публикации об эффективном использовании компьютерных методов и средств в целях зондирования и коррекции установок подсознания человека. Компьютер может выдать в очень быстром темпе визуальные и акустические сигналы (слова, фразы, образы). Сознательно человек воспринимать не успевает, но подсознание непроизвольно реагирует. Эти реакции компьютер через специальные датчики считывает и производит их обработку. В результате можно точно определить наличие в

подсознании человека определенной информации и личностных установок, причем даже такой, которая не фиксируется сознанием. Например, можно точно устанавливать патологические отклонения (наркоманию, половые извращения. психосоматические заболевания), факты прошлых событий (в том числе преступления) национальную принадлежность, родной язык, фамилии и имена близких и т.п. Все это безусловно негативно влияет жизнедеятельность человека, на его отношения к окружающему миру. В США, к примеру, существует закон, регулирующий доступ к информации и включающий следующие положения: передача информации есть общее правило, а не исключение; право на информацию является всеобщим; администрация обязана объяснить свой отказ предоставить требуемую информацию, тогда как запрос не должен быть мотивирован; лица которым было отказано в предоставлении информации, имеют право обратиться в суд. Первый закон по охране информации был принят в США в 1906 г. К настоящему времени там имеется более 500 законодательных актов по охране информации в части ответственности за ее разглашение и за компьютерные преступления.

По мере развития и усложнения средств и методов обработки, хранения и передачи информации по каналам связи повышается угроза потери ее конфиденциальности. Вопрос влияния информатизации на политическую власть является, пожалуй, центральным в западной политической жизни. Исследователи утверждают, что за счет концентрации информации, более широких возможностей ее использования происходит усиление исполнительной власти, власти государственного аппарата в сравнении с властью выборных представителей. Использование компьютерных сетей расширяет возможности аппарата в манипулировании массами.

Для России роль полной и достоверной информации в широком понимании многократно важнее, чем для многих других стран. Это объясняется двумя причинами: во-первых, процесс информационного взрыва, наряду с полезной и необходимой для развития общества информацией, заполнил информационное пространство необъективной, вредной, а часто преступно-опасной информации, отрицательно влияющей на образ мышления, культуру, уровень управления, нравственные и моральные основы общества, ставящие под сомнение саму государственность, суверенитет я территориальную целостность страны; во-вторых, рухнувший железный занавес превратил в значительной мере изолированное информационное пространство в геоинформационное. В силу этого вопросы внутренней и внешней информированности оказываются во взаимосвязи. Не трудно понять, что новые формы и условия хозяйствования, а также вопросы экологии, политики, социальной жизни, вооруженной защиты и многое другое носят более общественный, интернациональный характер. Эти два фактора, наряду с известными условиями современного бытия, ставят проблемы объективизации информации, государственного управления и его информационного обеспечения по-новому.

Опасный момент, связанный с информацией, - чрезмерная открытость нашего общества. Сейчас создается впечатление, что в стране нет никаких государственных тайн, и что строже всего охраняются секреты коммерческие. Информация должна иметь лимиты, обусловленные соображениями государственной безопасности, экономическими интересами страны, военными

задачами, наконец, нормами морально-этического порядка. Иногда газетная информация исполняет, по существу, роль "ликбеза" для террористов и преступников.. Серьезность вопроса обеспечения информационной безопасности требует ужесточения мер против тех, кто безответственно относится к представлению информации или, тем более, сознательно искажает ее.

Растущую опасность информационного плана для личности, общества, государства представляет новый тип социально опасных преступлений, основанных на использовании современно информационной техники и технологии. Основные виды этих преступлений включают махинации с электронными деньгами, компьютерное хулиганство, хищения разнообразной информации, хранящейся или передаваемой в "безбумажном" виде, незаконное её копирование и т.п..

Бурное развитие специальных технических средств нового типа, которые способны воздействовать на психику, сознание людей и на информационно-техническую инфраструктуру общества и армии, достигло такого уровня, что их характеризуют как новый вид оружия - электронное или информационное оружие. Это оружие включает различные средства нападения на компьютерные сети, начиная с электронного шпионажа до вирусов, способных разрушать ключевые системы. К нему относятся программные средства (компьютерные вирусы, программные закладки и пр.), средства радиоэлектронной борьбы, психотропные генераторы и т.д. Применение и разработка различных видов информационного оружия осуществляется все чаще и шире. Кое-где информационный терроризм стал элементом государственной политики. По данным ЦРУ США не менее 30 стран активно работают над компьютерными программами, являющими информационным оружием. Причем объектами для такого оружия все чаще становятся отдельные личности, социальные группы, а не только массы и государственные структуры, как это было не так давно. Иными словами, избирательность этого оружия растет. Отличительной чертой такого оружия является его дешевизна и сложность обнаружения. Система Интернет, связавшая компьютерные сети по всей планете, изменила правила, касающиеся современного оружия. Анонимность, обеспечиваемая Интернетом, позволяет противнику стать невидимым, обнаружить его очень сложно.

[Т (Ф.) Н.Цырдя, д-р филос. наук, проф., зав. кафедры философии и биоэтики ГУМФ им Н.А. Тестемицану РМ, академик Международной академии Информатизации при ООН, академик Укр. АИН, академик Международной академии Ноосферы (устойчивого развития)

А. Д. Урсул, д-р филос. наук, проф., директор Научно-исследовательского института устойчивого развития и безопасности, президент Международной академии Ноосферы (устойчивого развития), академик АН Молдовы и РАЕН, з.д.н. российской Федерации (г. Москва)]

Одним из средств обеспечения информационной безопасности являются отдельные нормы уголовного законодательства, содержащие составы преступлений, посягающие на информационные интересы личности, общества и государства, в частности, в частности, клевета (ст. 129 УК РФ), оскорбление (ст. 130 УК РФ), нарушение неприкосновенности частной жизни (ст. 137 УК РФ),

нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 138 УК РФ), разглашение тайны усыновления (удочерения) (ст. 155 УК РФ), заведомо ложный донос о совершении преступления (ст. 306 УК РФ); отказ в предоставлении гражданину информации (ст. 140 УК РФ), сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (ст. 237 УК РФ), государственная измена (ст. 275 УК РФ); шпионаж (ст. 276 УК РФ); возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ); разглашение государственной тайны (ст. 283 УК РФ); а также нормы главы 28 УК РФ.

6. Объектом преступлений, предусмотренных статьями 140 «Отказ в предоставлении гражданину информации» и 237 «Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей» Уголовного кодекса Российской Федерации, наряду со здоровьем, жизнью, имущественными интересами, является информационный интерес человека, то есть право на своевременное получение полной, достоверной информации в порядке, определенном соответствующим специальным законом.

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
(в ред. Федерального закона от 08.12.2003 N 162-ФЗ)

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами -

наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода

осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, -

наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, -

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, -

наказывается лишением свободы на срок до четырех лет.