ИНФОРМАЦИОННЫЕ ВЫЗОВЫ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Под общей редакцией

А.В. Федорова и В.Н. Цыгичко

Библиотека ПИР-Центра

Август 2001

УДК
ББК
И

Под общей редакцией:

к.ф.-м.н. А.В. Федорова и д.т.н., проф., академик РАЕН В.Н. Цыгичко.

Авторский коллектив:

д.ф.н. И.Ю. Алексеева, И.В. Авчаров, А.В. Бедрицкий, Д.С. Вотрин, д.в.н., проф. В.А. Дьяченко, В.Ф. Ильин, к.т.н. А.А. Кононов, д.и.н. А.В. Крутских, К.И. Мачабели, д.ф.н. Г.Л. Смолян, д.т.н., проф. А.А. Стрельцов, к.ф.-м.н. А.В. Федоров, д.т.н, проф., академик РАЕН Д.С. Черешкин, д.т.н., проф., академик РАЕН В.Н. Цыгичко.

Информационные вызовы национальной и международной безопасности/ И.Ю. Алексеева и др. Под общ. ред. А.В. Федорова, В.Н. Цыгичко. — М.: ПИР-Центр, 2001. — 328 с.

ISBN

Книга впервые в отечественной и зарубежной литературе на системной основе анализирует широкий круг проблем информационной безопасности и содержит некоторые рекомендации по ее обеспечению. В частности, в монографии рассматриваются новые угрозы безопасности в информационный век, информационное оружие и информационное противоборство, международно-правовые и политические аспекты информационной безопасности.

В приложения вошли глоссарий, обзор законодательств некоторых стран в области информационной безопасности, а также документы ООН по данной тематике.

Издание предназначено для широкого круга читателей включая политиков, дипломатов, военных, ученых, предпринимателей, исследователей и учащихся высших учебных заведений.

ISBN

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Всемирная федерация ученых в августе 2000 г. первой в списке угроз человечеству в XXI веке поставила угрозу информационной безопасности. Почему угрозы в информационной сфере вырвались вперед, обогнав экологию, энергетику и другие острые проблемы? И почему безопасность информационного пространства стала проблемой международной?

К концу XX века стремительное развитие и повсеместное внедрение новых информационных и телекоммуникационных технологий, являясь естественным этапом экономического и научно-технического прогресса и необходимым условием дальнейшего развития общества, породили одновременно комплекс негативных последствий.

Реальностью стала информационная и ее более известная форма — компьютерная преступность. Информационные технологии используются подчас деструктивными силами во внутриполитической борьбе.

Появилось информационное оружие, используемое против структур управления государством, экономикой и вооруженными силами. Информационное оружие меняет не только методы ведения военных действий, меняется самое понятие войны, стираются грани между военным и мирным временем, пропадает устоявшееся восприятие понятий «театр военных действий», еще более сращиваются военные и мирные технологии, расширяется понятие «оружие». Появляется возможность выиграть войну без нанесения физического ущерба и проникновения на территорию противника. Исключительно опасно использование подобных средств террористическими и экстремистскими организациями.

До сих пор, однако, разработка, производство, распространение и применение информационного оружия не регулируются международным правом. Три принятые Генеральными Ассамблеями ООН (в 1998-2000 гг.) по инициативе России резолюции, хотя и привлекли внимание к проблеме информационной безопасности, не стали основанием для принятия конкретных шагов по подготовке международного документа, останавливающего гонку вооружений в информационной сфере. Констатировали опасность, но пока воздерживаются от конкретных ответов на новый вызов другие крупные международные форумы, такие как: «большая восьмерка», ОБСЕ, «Шанхайская организация сотрудничества».

Похоже, широкие круги мировой общественности, политической и интеллектуальной элиты не в полной мере осознали значение международной информационной безопасности и опасность информационных войн. До сих пор в данной области нет общепринятого понятийного аппарата, развернутой классификации угроз информационной безопасности, не оценивались их конкретные последствия, не разработаны основы классификации и принципы идентификации различных видов информационного оружия.

Вместе с тем в последние годы сложился, пусть пока немногочисленный, круг специалистов различных российских государственных ведомств и научных учреждений, выработавший согласованный взгляд на проблему информационной безопасности. Он лег в основу российских инициатив в ООН и государственных документов по вопросам информационной безопасности.

Стремлением сделать еще один шаг в разработке проблем информационной безопасности продиктовано издание настоящей монографии. Она подготовлена коллективом экспертов авторитетных государственных и научных учреждений. В ней предпринята попытка охарактеризовать основные аспекты проблемы и дать необходимые сведения, в том числе справочного характера.

Книга могла бы оказать помощь государственным деятелям и общественности в понимании основных аспектов проблемы информационной безопасности как в национальном, так и в международном ее измерениях, а также в осознании тех конкретных опасностей, которые возникают при использовании достижений в информационной сфере в качестве оружия.

Кроме того, это издание могло бы служить источником информации по проблеме обеспечения международной информационной безопасности и отдельным ее аспектам для политиков, дипломатов, военных, научных работников и представителей бизнеса, а также государственных и общественных организаций.

Авторы благодарны коллективу ПИР-Центра и особенно его руководителю Орлову В.А. за поддержку в подготовке и оперативное издание монографии. Кроме того, авторы выражают благодарность начальнику управления Совета Безопасности Российской Федерации Г.В. Емельянову за сделанные замечания и ценные предложения.

ОБРАЩЕНИЯ К ЧИТАТЕЛЯМ

Уважаемые читатели!

России принадлежит инициативная роль в официальной постановке перед ООН идеи обеспечения режима международной информационной безопасности. В известном письме Генеральному секретарю ООН 23 сентября 1998 г. с российской стороны акцентировалась необходимость учитывать, возможно, пока и потенциальную, но от этого не менее серьезную опасность использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности и безопасности, соблюдением принципов неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека. На наш взгляд, такая опасность уже сейчас требует принятия превентивных мер. Нельзя допустить возникновения принципиально новой области конфронтации на международной арене, способной спровоцировать новый виток гонки вооружений на основе достижений научно-технической революции и в итоге отвлечь огромные ресурсы, так необходимые для целей мирного созидания и развития.

С удовлетворением отмечаю, что предметное и целенаправленное обсуждение в рамках ООН темы международной информационной безопасности имеет положительную динамику. Третий год подряд предлагаемые Россией политические резолюции по этой проблематике под общим названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» получают консенсусное одобрение в ходе голосований на Генеральной Ассамблее ООН. Столь широкая поддержка российской инициативы стала возможной благодаря тому, что последняя носит объективно конструктивный и неконфронтационный характер.

Тема создания глобального информационного общества, в котором была бы прочно гарантирована международная информационная безопасность, стала одной из важнейших составляющих международных отношений XXI века, предметом тщательного рассмотрения многих мировых форумов, включая «восьмерку». Активно она ставится Россией в контексте ее двусторонних переговоров от экспертного до самого высшего государственного уровня с другими странами.

Мы видим возможность продвижения идеи международной информационной безопасности на основе поэтапного подхода,

расширения географии и сфер обсуждения проблемы, постепенного наполнения последующих резолюций ООН и решений других международных форумов конкретизирующими положениями, отвечающими общим интересам международного сотрудничества, безопасности и стратегической стабильности.

Хотел бы выразить надежду, что исследовательская работа российских специалистов поможет читателям лучше понять суть проблемы информационной безопасности, осознать угрозы, которые несет с собой применение новых информационных технологий в военных, криминальных, террористических и всех других противоправных целях.

Заместитель Министра иностранных дел Российской Федерации — Г. Мамедов

Уважаемые читатели!

Стержнем и одним из определяющих факторов развития человечества в XXI веке становятся информация и, соответственно, информационные технологии. Мировая информационно-технологическая революция радикально изменила политику, экономику и социальную жизнь планеты. Позитивная сторона этих перемен очевидна. Увы, приходится заострить внимание на потенциальных угрозах, связанных с информационно-технологическим прогрессом. Вот лишь некоторые из них: информационный терроризм, вмешательство в частную жизнь, информационный криминал, и, наконец, чреватое катастрофическими последствиями использование информационных технологий в военных целях.

На парламентариях всех стран лежит особая ответственность — обеспечить адекватную правовую основу противодействия этим новым вызовам, в частности, путем гармонизации национальных законодательств с целью обеспечения исключительно законного использования информационных средств и технологий, а также международной информационной безопасности. При этом регламентация использования национального и международного информационного пространства ни при каких условиях не должна подрывать один из фундаментальнейших принципов демократии — свободу слова и доступа к информации.

Председатель Комитета по международным делам Государственной Думы Федерального Собрания Российской Федерации — Д. Рогозин

Уважаемые читатели!

Человечество вступило в новую стадию своего развития, связанную с формированием постиндустриального общества, часто называемого «информационным обществом».

Политическая программа формирования глобального информационного общества закреплена в Окинавской хартии 2000 г., подписанной руководителями восьми развитых стран мира. Свою подпись под этим документом поставил и Президент Российской Федерации В.В. Путин.

В Окинавской хартии отмечено, что информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, взаимодействия правительства и гражданского общества. Информационные технологии быстро становятся жизненно важным стимулом развития мировой экономики.

Важным направлением формирования информационного общества является обеспечение его безопасности, которая может быть достигнута только тогда, когда будет обеспечена безопасность национальных информационных инфраструктур каждой страны мира, а также глобальной информационной инфраструктуры в целом как технологической основы мирового информационного пространства.

В резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», принятой в декабре 2000 г., содержится призыв к государствам-членам содействовать рассмотрению на многостороннем уровне не только угроз в сфере информационной безопасности, но и возможных мер по ограничению этих угроз.

Думаю, что настоящая книга будет способствовать достижению этой цели.

Первый заместитель Секретаря
Совета Безопасности
Российской Федерации — В. Шерстюк

ВВЕДЕНИЕ

Термин «информационная безопасность» появился в России в 1992 г. после принятия закона Российской Федерации «О безопасности». Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 6 сентября 2000 г., определяет это понятие как состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Имеется в виду, что:

- интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность;
- интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России;
- интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Исходя из этого, можно рассматривать обеспечение информационной безопасности как противодействие враждебному воздействию на важнейшие информационные системы государств, использованию информационных систем в преступных целях, наиболее опасной формой которых является кибертерроризм.

Включение «информационной» компоненты в структуру понятия «безопасность» обусловлено тем, что устойчивое развитие информационных систем является одним из ключевых факторов развития российского общества, во многом определяющем успешное осуществление его социально-политического и экономического переустройства на демократической основе.

Это связано с несколькими обстоятельствами.

Глобализация стала важнейшей тенденцией развития современного мира, и страны, отгораживающиеся от этого процесса, окажутся на обочине развития цивилизации. Технологической основой глобализации стали интеграция информационных систем различных государств в единую общемировую информационную сферу, формирование единого информационного пространства, создание глобальных информационно-телекоммуникационных сетей, интенсивное внедрение новых информационных технологий во все области человеческой деятельности.

Так, по данным ЮНЕСКО, в развитых и развивающихся странах мира длительное время сохраняется позитивная динамика развития телекоммуникационных систем и соответствующих рынков капитала. В частности, с 1995 по 2000 г. число телефонных линий увеличилось в США — с 165 тыс. до 199 тыс., в ФРГ — с 41 тыс. до 51 тыс., в Китае — с 41 тыс. до 241 тыс., в России — с 25 тыс. до 30 тыс. Одновременно количество телефонных линий на каждые 100 жителей увеличилось в США — с 63 до 72, ФРГ — с 49 до 63, в Китае — с 3 до 19, в России — с 17 до 20. За это же время в развитие телекоммуникационной инфраструктуры инвестировано в США — 51 млрд долл., в ФРГ — 16 млрд долл., в Китае — 302 млрд долл., в России — 8 млрд долл.[1]

Количество абонентов сотовых телефонных сетей в мире только за 1997 г. увеличилось с 70 млн до 207 млн, а к 2003 г. может возрасти до 830 млн.

Ошеломляющими темпами растет количество пользователей интернета, ставшей главной информационной системой мира. Если в 1993 г. оно не превышало 70 тыс. человек, то к концу 2001 г., как ожидается, оно достигнет 500 млн человек. Активно развивается этот сектор информационной инфраструктуры и в России, в которой число зарегистрированных пользователей интернета на начало 2000 г. составляло около двух миллионов человек[2].

При этом, интенсивное развитие информационной инфраструктуры является технологической основой преобразования практически всех сторон жизни современного общества, экономики, образования, культуры. Оно «раскрепощает» человека, расширяет его возможности, содействует

[1] Всемирный доклад по коммуникациям и информации 1999-2000. Polpred ASBM: 5-900034-10-0. Париж, ЮНЕСКО, 2001.

[2] Комментарий к российскому изданию Всемирного доклада по коммуникациям и информации 1999-2000. Polpred ASBM: 5-900034-10-0. Париж, ЮНЕСКО, 2001.

освобождению от окаменелых идеологических догм, увеличивает потенциал социальной адаптации, активности и самореализации.

В итоге, быстрыми темпами расширяется создание, производство и потребление информационных технологий. Эти сегменты экономики оказывают растущее влияние на экономическую жизнь общества в целом. Так, в США расходы на современные информационные технологии как составляющую производственного оборудования увеличились с 5% в 1960 г. до 45% в 1996 г. По оценке Министерства торговли США, в 1998 г. промышленность, имеющая отношение к информационным технологиям, произвела продукции и услуг на 683 млрд долл. В некоторых промышленно развитых странах доля валового внутреннего продукта (ВВП), связанная с деятельностью в сфере современных информационных технологий, составила в 1997 г. почти 8%, а его соответствующий прирост — свыше 12%. На долю информационных технологий приходится от 10 до 15% от общего объема мировой торговли. Все возрастающая экономическая значимость современных информационных технологий в определенной степени связана и с ростом электронной торговли. В 1998 г. она принесла 26 млрд долл. прибыли и ожидается, что в начале XXI века эта цифра превысит триллион долларов[3].

Достижения России в этой области намного скромнее. Однако можно говорить об определенном влиянии информационных технологий на российскую экономику. Так, объем российского рынка информационных технологий, после финансового кризиса августа 1998 г., составлял около двух миллиардов долларов.

Индустрия информатизации, телекоммуникации и связи, информационных услуг является сегодня одной из наиболее динамичных сфер мировой экономики, способной конкурировать по доходности с топливно-энергетическим комплексом, автомобилестроением, производством сельскохозяйственной продукции. От нее во многом зависит наукоемкость промышленной продукции и ее конкурентоспособность на мировом рынке.

Далее, утверждение свободы информационной деятельности в качестве общепризнанной нормы международного права и, как следствие, неизбежное сужение возможностей государств ограничивать свободу этой деятельности, наряду с интенсивным развитием новых средств доступа к информации, привело к усилению роли общественных институтов,

[3] Всемирный доклад по коммуникациям и информации 1999-2000. Polpred ASBM: 5-900034-10-0. Париж, ЮНЕСКО, 2001.

прежде всего средств массовой информации (СМИ), в формировании государственной политики.

Влияние СМИ в формировании государственной политики во многом связано с тем, что в современном обществе они выполняют как бы роль посредника между гражданами и государством, обеспечивают возможность ведения диалога между обществом и властью, являются действенным фактором формирования общественного мнения по наиболее важным проблемам внутренней и внешней политики. Кроме того, свободное функционирование СМИ способствует обеспечению общественного контроля за деятельностью государства, его отдельных институтов, органов и должностных лиц. В свою очередь, через СМИ государство разъясняет гражданам те цели, которые оно перед собой ставит, выбираемые методы достижения этих целей, успехи и неудачи на этом пути.

Наконец, и это самое главное, широкое внедрение современных информационных технологий во все сферы общественной жизни, в материальное производство и вооруженные силы усиливает зависимость общества и государства от устойчивой работы информационных и телекоммуникационных систем, сетей связи, сохранности информационных ресурсов, являющихся важной составной частью информационной инфраструктуры общества.

Сбои в работе информационных и телекоммуникационных систем могут привести к катастрофическим последствиям. Человечество в полной мере осознало это в связи с так называемой «Проблемой-2000». Возникла ситуация, чреватая тем, что «технологические недоработки» могли привести к «параличу» всей инфраструктуры современного общества. Пессимисты предсказывали даже возможность несанкционированного начала ядерной войны. Для предотвращения негативных последствий проявления «Проблемы-2000» человечество вынуждено было заплатить гигантскую сумму, которая, по некоторым оценкам, составляет около 500 млрд долл.

По мере того, как растет значение и роль информационных и телекоммуникационных систем, возрастает опасность тяжелых последствий в результате несанкционированных воздействий на такие системы и сети связи со стороны преступных групп. Если в 1997 г. ФБР США вело расследование по 200 случаям компьютерных преступлений, то в 1999 г. это число превысило 800.

Стремительно растет угроза компьютерной преступности в России. За последние три года общее количество зарегистрированных преступлений в сфере компьютерной информации возросло более чем в 63 раза, почти в 30 раз возросло количество преступлений, связанных с неправомерным доступом к компьютерной информации; в 137 раз — с созданием, использованием и распространением вредоносных программ для ЭВМ; в 75 раз — с незаконным производством, сбытом или приобретением в целях сбыта специальных технических средств, предназначенных для негласного получения информации[4].

Иными словами, информационная сфера становится все более важным фактором устойчивого функционирования и дальнейшего развития общества. Человечество вплотную подошло к качественному рубежу, связанному с возникновением «информационного общества».

Несмотря на широкое использование этого термина ученые и специалисты пока не пришли к единому пониманию его содержания. Одни считают, что это общество, в котором обеспечивается «легкий и свободный доступ к информации по всему миру», другие — что это общество, в котором «основными объектами и результатами труда» большинства являются информация и знания.

Представляется, что более правы те, кто считает, что если речь идет о некоторой новой стадии развития общества, ее более правильно определять на основе анализа изменения производительных сил и производственных отношений. С этой точки зрения информационное общество может быть определено как общество, в котором основным предметом труда большей или значительной части людей являются информация и знания, а орудием труда — информационные технологии.

Интенсивное развитие «информационной» экономики и эффективное использование интеллектуальных ресурсов расширят возможности индивида раскрыть свои потенциальные способности и реализовать свои убеждения.

Складывающиеся в информационном обществе социальные отношения, видимо, во многом будут определяться именно этими обстоятельствами. Соответственно, его экономика будет, прежде всего, ориентирована на производство продуктов информационной и интеллектуальной деятельности,

[4] Егоров Иван. Совбез: «Правила игры для всех СМИ должны быть одинаковы». Интервью с начальником управления аппарата Совета Безопасности РФ Г.В. Емельяновым. *www.strana.ru/security/state/2001/02/981140788.htm*.

связанных с выработкой новой информации и новых знаний, преобразованием их к виду, удобному для потребления другими людьми, и продажей этих продуктов. Следствием этого будет формирование новых экономических, культурных и социальных стандартов, обусловленных, в частности, уровнем информатизации общественной жизни, включая образование и культуру, управление государством, осуществление научных исследований и интегрированностью государства и общества в мировое сообщество.

Формирование информационного общества не может быть осуществлено усилиями одной, даже самой развитой страны. Именно поэтому руководители «восьмерки» наиболее развитых стран приняли в 2000 г. Окинавскую хартию глобального информационного общества, в которой закреплены принципы международного сотрудничества в этой области. В частности, подписавшие Хартию главы государств подтвердили «приверженность принципу участия в этом процессе: все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества»[5].

Экономические, политические и социальные выигрыши, которые сулит переход из индустриального общества в постиндустриальное (как часто называют информационное общество), делают эту задачу одной из доминант национальных интересов многих стран мира.

В условиях информационного общества выживание, экономическое процветание, поддержание социальных и политических ценностей общества во все большей степени связаны с развитием информационной сферы, а также с нейтрализацией угроз возникающих в связи с растущей уязвимостью социума и материального производства от теснейшего функционирования информационных систем.

Среди них не последнее место занимают угрозы, связанные с тем, что информационная инфраструктура, информационные ресурсы во все большей степени становятся ареной межгосударственного противоборства. Существенную опасность представляют разрабатываемые средства «силового» воздействия на информационно-телекоммуникационную инфраструктуру противостоящих государств, несанкционированного доступа к их информационным и телекоммуникационным ресурсам. К сожалению, уже вошли в обиход, хотя и не получили точных дефиниций, в том числе в международном

[5] Окинавская хартия глобального информационного общества. Документы встречи «большой восьмерки». Окинава, 22 июня 2000 г.

праве, такие понятия, как «информационная война», «информационное противоборство», «информационная операция»и т.п.

Данные обстоятельства делают обеспечение безопасности интересов Российской Федерации в информационной сфере важным фактором национальной безопасности в целом.

Можно выделить несколько основных источников угроз безопасности информационного общества, которые могут затрагивать интересы человека, общества и государства.

Интересы человека, которые необходимо охранять в информационном обществе, заключаются, прежде всего, в реальном обеспечении конституционных прав и свобод гражданина на доступ к открытой информации, на использование информации в интересах осуществления не запрещенной законом деятельности, а также в защите информации, обеспечивающей личную безопасность, духовное и интеллектуальное развитие.

Важной особенностью образа жизни в информационном обществе будет существенное сокращение «информационных» расстояний (времени доступа к требуемой информации), что приведет к появлению новых возможностей — как по формированию личности, так и реализации ее потенциала. Человечество вплотную подходит к рубежу, за которым информационная инфраструктура становится, по существу, основным источником информации для человека, оказывает непосредственное влияние на его психическую деятельность, на формирование его социального поведения.

Сложность современных информационных технологий критически увеличивает зависимость человека от других людей, осуществляющих разработку таких технологий, создающих алгоритмы поиска требуемой информации, ее предварительной обработки, приведения к виду, удобному для восприятия, доведение до потребителя. По существу, эти люди во многом формируют информационный фон общества и индивида, определяют субъективную оценку условий, в которых он живет и действует, решает свои жизненные проблемы. Именно поэтому представляется исключительно важным обеспечить безопасность взаимодействия человека с информационной инфраструктурой.

Другим опасным источником угроз интересам человека является использование во вред его интересам персональных данных, накапливаемых органами государственной власти, а также расширение

возможности скрытого сбора информации, составляющей его личную и семейную тайну, сведений о его частной жизни.

Это обусловлено, на наш взгляд, трудностями реализации механизмов охраны этих сведений, дальнейшими успехами в области миниатюризации средств скрытого сбора и передачи информации.

Интересы общества в информационной сфере заключаются в защите жизненно важных интересов личности в этой сфере, обеспечении реализации конституционных прав и свобод человека и гражданина в интересах упрочения демократии, достижения и поддержания общественного согласия, повышения творческой активности населения.

Одним из источников угроз интересам общества в информационной сфере является непрерывное усложнение информационных систем и сетей связи критически важных инфраструктур обеспечения жизни общества.

Эти угрозы могут проявляться в виде как преднамеренных, так и непреднамеренных ошибок, сбоев и отказов техники и программного обеспечения, вредного воздействия на эти инфраструктуры со стороны преступных структур и криминальных элементов. Объектами реализации таких угроз могут выступать информационные системы энергетической, транспортной, трубопроводной и некоторых других инфраструктур.

Масштаб возможных последствий сбоев и ошибок в работе технического и программного обеспечения информационных систем до некоторой степени можно представить по затратам на решение «Проблемы-2000».

Наконец, опасным источником угроз является расширение масштабов отечественной и международной компьютерной преступности.

Угрозы могут проявляться в виде попыток осуществления мошеннических операций с использованием глобальных или отечественных информационно-телекоммуникационных систем, отмывания финансовых средств, полученных противоправным путем, получения неправомерного доступа к финансовой, банковской и другой информации, которая может быть использована в корыстных целях.

Одним из наиболее опасных источников угроз интересам общества и государства в информационной сфере являются неконтролируемое распространение «информационного оружия» и развертывание гонки

вооружений в этой области, попытки реализации концепций ведения «информационных войн». Разрушительное воздействие «информационного оружия» в информационном обществе может оказаться более мощным и эффективным, чем это представляется сегодня.

В Окинавской хартии отмечено: «Задача создания предсказуемой, транспарентной и недискриминационной политики и нормативной базы, необходимой для информационного общества, лежит на правительствах». Данный принцип, на наш взгляд, имеет отношение и к обеспечению безопасности технологической основы информационного общества. Руководители государств, подписавшие Хартию, закрепили необходимость «разработки эффективных национальных и международных стратегий» формирования информационного общества, включая вопросы «борьбы со злоупотреблениями, которые подрывают целостность сети», а также «согласованных действий по созданию безопасного и свободного от преступности киберпространства», поиска «эффективных политических решений актуальных проблем, как, например, попытки несанкционированного доступа и компьютерные вирусы». Это создает основу для создания эффективной системы обеспечения международной информационной безопасности, снижения риска превращения информационной сферы в арену противоборства между государствами в целях разрешения политических противоречий.

Можно выделить несколько основных направлений осуществления подготовительной работы по формированию системы международной информационной безопасности:

- совершенствование национального законодательства, регулирующего отношения в информационной сфере, и системы международных договоренностей по вопросам противодействия угрозам безопасности информационного общества;
- совершенствование системы организации правоохранительной и судебной деятельности в области обеспечения безопасности законных интересов граждан, общества и государства в информационной сфере как на национальном, так и на международном уровне;
- совершенствование технологического обеспечения безопасности информационной инфраструктуры, средств защиты информации, проведения оперативно-следственных мероприятий, включая их нормативное обеспечение;
- совершенствование системы подготовки кадров для реализации функций обеспечения безопасности информационной сферы общества;
- создание системы культурно-образовательного обеспечения безопасности информационной сферы.

ГЛАВА 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — ФАКТОР МЕЖДУНАРОДНОЙ ПОЛИТИКИ

По мере формирования информационного общества глобальное соотношение сил во все большей мере будет определяться способностью внедрения информационных систем и технологий в экономические, военные, технологические и культурные сферы общества.

Международно-политические последствия информатизации

XX век вошел в историю как период колоссальных изменений, связанных прежде всего с быстрым научно-техническим и технологическим развитием. Неотвратимо проявляется мультипликативный эффект открытий и изобретений в области обработки информации и коммуникации. И каждый информационно-технологический прорыв оказывается все более глобальным, изменяющим облик цивилизации.

Изменение мирового информационного пространства стало ключевым фактором развития современной цивилизации и определяет основные направления общественного развития. К наиболее важным из них относятся:

- ускорение научного, научно-технического, экономического, социального, культурного и других направлений развития за счет увеличения объема и скорости информационного обмена вне зависимости от расстояния, возможности распространения новых идей и знаний, быстрого распространения научных и технологических достижений;
- создание базы для разработки и распространения новой научной и философской парадигмы XXI столетия, основанной на понимании единства многообразия мира и осознании общих глобальных проблем человечества;
- усиление мировых интеграционных тенденций, особенно в экономической, политической, информационной, научно-технической, образовательной, культурной и других сферах;
- создание условий для разработки и внедрения новых форм и методов обеспечения глобальной, региональной и национальной безопасности;
- прогресс в области политического, экономического, производственного и военного управления и международных отношений.

Всеобщая информатизация, как глобальный фактор мирового развития, оказывает существенное влияние на международно-политическое

положение и будущее каждой страны, которое во многом определяется уровнем развития транспортной, информационной и технологической инфраструктуры. Все они, в свою очередь, зависят от современной информационной инфраструктуры, которая, в частности, создаст базу для развития инвестиционного процесса и, соответственно, для ускоренного экономического и социального развития и занятия достойного места в мировом хозяйстве.

Развитие мира после «холодной войны» весьма противоречиво. С одной стороны, углубляется глобальная экономическая и технологическая взаимозависимость, чему способствует развитие мирового информационного пространства. С другой — сохраняются межгосударственные противоречия, источники международной нестабильности и конфликтов, многие из которых, особенно в зоне «третьего мира», обостряются и становятся все более масштабными. В быстро развивающемся и приобретающем принципиально новые качества мировом информационном пространстве традиционные методы межгосударственного противоборства трансформируются под воздействием новых информационных технологий и становятся все более опасными.

Развитие информатизации порождает комплекс негативных международно-политических последствий. Прежде всего это ускорение поляризации мира, увеличение разрыва между богатыми и бедными, технологически отсталыми и передовыми странами во всех областях, увеличение числа стран маргиналов, а также так называемых «рухнувших государств». Это является главным источником нестабильности, сегодняшних и будущих конфликтов, в том числе могущих обрести глобальные масштабы. Резко увеличивается военный потенциал передовых в научно-техническом отношении стран, приводящий к изменению глобального и региональных балансов сил. Это может провоцировать озабоченность и даже враждебную реакцию «отстающих» государств, поражая таким образом новые очаги противостояния.

Иными словами, информатизация не только ускоряет развитие цивилизации, но и порождает новые угрозы национальной, региональной и глобальной безопасности.

Весьма глубокими являются изменения, происходящие под воздействием новых информационных технологий в военной сфере. Их широкое внедрение значительно увеличивает боевые возможности традиционных видов вооружения и военной техники. Качественно изменяются

возможности разведки и связи, во много раз увеличиваются скорости обработки больших массивов информации и принятия решений, что позволяет перейти к принципиально новым методам управления войсками и оружием на всех уровнях от стратегического до тактического.

Новые информационные технологии позволили резко увеличить боевые возможности средств радиоэлектронной борьбы и создать информационное оружие. Информационно-технологический прогресс (иногда его называют информационной революцией) в военном деле, способствующий резкому увеличению боевых возможностей войск ведет не только к изменению форм и способов ведения боевых действий различного масштаба, но изменяет саму традиционную парадигму вооруженной борьбы от тактического до стратегического уровня. Появление информационного оружия принципиально меняет механизм эскалации вооруженных конфликтов. По мнению многих экспертов, даже выборочное применение информационного оружия по объектам военной и гражданской информационной инфраструктуры может завершить конфликт на его ранней стадии, т.е. до начала активных боевых действий, т.к. эскалация информационного воздействия ведет к катастрофе. Обладание информационным оружием обеспечивает военное преимущество над странами его не имеющими. Уже в ближайшем будущем информационно-психологические параметры противостояния держав могут доминировать над ядерными. При этом, как и ядерное, информационное оружие может служить как фактором политического давления, так и фактором сдерживания.

Информационное оружие как инструмент силовой политики

Активная разработка информационного оружия и подготовка к информационным войнам во многом определяются взглядами развитых стран на цели, условия, формы и последствия применения военной силы.

Становление в развитых демократических странах гражданского общества как важной социально-политической силы, осуществляющей общественный контроль над властью, стимулировало формирование новой системы ценностей, в которой ключевое значение имеет жизнь человека, его права и безопасность. Развитие гражданского общества имеет устойчивую, необратимую тенденцию к углублению и распространению на все более широкий круг стран. Для гражданского общества неприемлем военный путь решения внешнеполитических

проблем, если боевые действия связаны со значительными людскими потерями, если только не возникает угрозы существованию общества и государства. Использовать же военную силу, в ситуациях не угрожающих существованию этих государств, становится все сложнее по мере развития гражданского общества.

Опыт военных конфликтов в последнее десятилетие говорит о том, что уровень допустимых для демократических государств потерь составляет сегодня десятки, если не единицы, человеческих жизней и это становится одним из важнейших факторов сдерживания этих стран от применения военной силы.

Далее, глобализация и, особенно, растущее совпадение экономических и политических интересов развитых демократических стран, исключают военные конфликты между ними. Их общие интересы требуют, помимо всего прочего, надежного обеспечения безопасности каждого члена «клуба» и возможности совместного решения острых мировых проблем, в том числе с применением силы. Эту задачу выполняют военные союзы этих стран, в которых решения принимаются по принципу консенсуса. В этих условиях без поддержки общественного мнения стран-участниц союза невозможно решение каких-либо проблем военным путем. Это обстоятельство резко снижает возможности военных организаций союзов развитых демократических стран в операциях, не затрагивающих напрямую их безопасность. Поэтому основными средствами решения острых политических проблем стали экономическая и культурная экспансии, международные экономические и политические санкции и в крайних случаях угроза применения силы там, где это не грозит серьезными людскими потерями с обеих сторон. В этих условиях информационное оружие может стать весьма эффективным силовым средством, позволяющим решать многие конфликты без применения традиционных средств вооруженной борьбы.

Эти тенденции развиваются на фоне увеличения уязвимости промышленной, информационной, социальной и военной инфраструктуры развитых стран. Разрушение в результате боевых действий атомных электростанций, химических предприятий, высоконапорных плотин и других критических объектов может привести к региональным и даже глобальным катастрофам, чреватыми колоссальными людскими и материальными потерями, грозящими самому существованию этих стран. Нарушение их информационной инфраструктуры также приведет к техногенным и экономическим катастрофам, поскольку управление всеми

важнейшими объектами народного хозяйства, социальной и военной сферы развитых стран основано на широком использовании информационно-коммуникационных технологий. Дальнейшее развитие информационно-коммуникационной сферы и углубление глобализации делает мир еще более уязвимым.

Наконец, информационно-технический прогресс в военном деле, создает условия для ускоренного совершенствования вооружения и военной техники на основе широкого внедрения новых информационных технологий и создания оружия на новых физических принципах, информационного и нелетального оружия. Основными особенностями нового поколения вооружений становятся кардинальное увеличение точности, дальности и мощности действия, резкое увеличение возможностей разведки, систем сбора и обработки информации и, как следствие, уменьшение времени принятия оперативных решений. Страны, обладающие таким оружием и военной техникой, получают громадное военное преимущество перед противником, оснащенным традиционными типами вооружений.

Перечисленные тенденции, по сути, и определяют допустимые пределы и условия применения силы развитыми странами и возможные типы конфликтов, которые могут быть для них приемлемы.

В частности, для развитых стран неприемлема какая-либо война с применением ядерного оружия. Как следует из выступлений американских политиков и военных, отстаивающих необходимость создания национальной ПРО, уровень недопустимого ущерба в ядерном конфликте для США определяется ущербом любому мегаполису от одной боеголовки самой малой мощности.

Проблематичным становится и развязывание широкомасштабной войны с применением обычного оружия против противника, который способен оказать серьезное сопротивление, чреватое для агрессора большими людскими потерями и серьезным ущербом инфраструктуре. В настоящее время и, очевидно, в будущем не существует политических и экономических причин, ради которых Запад мог бы развязать войну, угрожающую его экономическому процветанию, обеспеченной и безопасной жизни его граждан.

Опыт последних десятилетий показывает, что после окончания вьетнамской войны США и НАТО применяли силу только в случае, если

они имели подавляющее военно-техническое превосходство над противником, который не мог создать для них непосредственной угрозы.

Из этого следует вывод, что превентивное применение военной силы развитыми странами возможно только при их подавляющем военно-техническом превосходстве над противником, а информационное оружие становится наиболее приемлемым военным средством борьбы.

Угроза международного информационного терроризма

Процессы глобальной информатизации привели к тому, что современное общество все более полно зависит от состояния своей информационной инфраструктуры. Это делает его весьма уязвимым, а также позволяет воздействовать на него враждебным силам — недружественным государствам, террористическим организациям, криминальным группам и отдельным злоумышленникам.

Поскольку угрозы информационного терроризма могут быть направлены на любые сферы жизни общества и государства, на любые объекты киберпространства, необходима разработка единой общемировой стратегии борьбы с информационным терроризмом, в соответствии с которой функции силовых ведомств каждого государства должны быть четко распределены, а государство должно координировать их деятельность.

Стратегия борьбы с информационным терроризмом должна строиться на основе поиска приемлемого для общества компромисса, быть открытой, не допускающей монополизма отдельных ведомств.

ГЛАВА 2. НОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫЙ ВЕК

Преступность в информационной сфере

Как и любое достижение науки и техники, информационно-телекоммуникационные технологии могут использоваться и используются не только в общественно-полезных, но и в противоправных, в том числе в криминальных целях. Об информационном терроризме уже упоминалось выше. Но есть и просто криминальные действия, осуществляемые в отношении информационных ресурсов или с их использованием. В их числе можно выделить неправомерное получение конфиденциальной информации, денежных средств, уклонение от уплаты налогов и т.д. Число компьютерных преступлений в последнее время стремительно растет, что вызвано повышением доступности как программно-аппаратных средств, так и необходимых знаний и умений. В частности, киберпреступность становится одним из основных источников угроз для только становящегося российского бизнеса.

Информационный криминал

Наиболее «известными» и «популярными» преступниками в информационном пространстве в последние годы стали хакеры. Это, как правило, специалисты в области информационных технологий, освоившие их в основном самостоятельно. Социопсихологической основой их деятельности является то, что полученные ими знания и способность достаточно свободно ориентироваться в информационном пространстве выступают как компенсация за некоторую их социальную изолированность — недостаток общения в обычной жизни они восполняют общением в мире виртуальном. Их противоправные действия нередко не имеют корыстного умысла, доступ к компьютерной информации совершается с целью самоутверждения, приобретения авторитета среди единомышленников или из хулиганских побуждений. Деятельность по проведению информационных атак на компьютерные системы часто расценивается ими как своего рода искусство.

Действия хакеров могут быть связаны с их личностными особенностями, в частности с комплексом неполноценности, который они пытаются преодолеть, бросая вызов обществу. Исследования показали, что большинство «компьютерных пиратов» — это молодые люди немногим старше 20 лет, испытывавшие затруднения в межличностных отношениях.

Как правило, они плохо успевали в школе, но сумели добиться успехов в области вычислительной техники посредством самообразования, проявляя огромное терпение и маниакальное пристрастие к компьютерным технологиям. Часто они увлекаются идеями анархизма, трактуя их, в частности, как полную свободу действий в информационном пространстве. Такие психологические качества и идейные установки могут сформировать в хакере агрессивность и подтолкнуть его к актам террора национального или международного масштаба.

В последнее время наметилась тенденция объединения хакеров в группировки, в рамках которых они обмениваются знаниями, умениями, полученной в сети информацией. Кроме того, сообща легче совершать преступления, так как можно задействовать более мощные информационные ресурсы. В группы могут входить специалисты разных областей: знающие особенности уязвимости конкретных операционных систем, средств защиты, сетевых протоколов и т.д. Нередко члены этих группировок не знают друг друга реально, а общаются, используя возможности открытых коммуникационных сетей.

Необходимо отметить, что хакеры совершают компьютерные преступления далеко не всегда самостоятельно. В преступном мире происходит осознание того, что без знания современных информационных технологий практически невозможно завладеть финансовыми средствами, получить необходимую информацию. Кроме того, компьютерные преступления, как правило, оставляют гораздо меньше следов, требуют небольших временных и материальных затрат. Все это делает новые информационных технологии удобным орудием совершения самых разнообразных преступлений.

В этой связи преступные группировки активно изучают компьютерные технологии, привлекают к своей деятельности специалистов в этой области. Как правило, последними выступают не имеющие прочных моральных принципов подростки и молодые люди, которые приобрели знания самостоятельно или в период учебы в высшем учебном заведении и ищут себе применение. Преступные группировки предлагают этим специалистам достаточно большие деньги, нередко используя идеи анархизма и абсолютной свободы в информационном пространстве.

В числе компьютерных преступлений значительную долю (около 40%) составляют правонарушения, целью которых является получение информации ограниченного доступа. Большое распространение они

получили в связи с тем, что в последнее время повсеместно в производственные процессы, управленческую, банковскую, коммерческую деятельность, в другие сферы общественной жизни внедряются средства вычислительной техники. Там накапливается большое количество информации, в том числе конфиденциального характера.

Объектами такого рода преступлений являются чаще всего базы и банки данных, компьютерные сети органов государственной власти, органов власти субъектов федерации и местного самоуправления, организаций, предприятий и учреждений, а также частных лиц. Как правило, эти действия являются составной частью промышленного шпионажа, суть которого состоит в неправомерном получении информации коммерческого и иного характера в отношении своих конкурентов.

Другая менее заметная часть преступных посягательств имеет целью не просто получение доступа к некоторой информации, а ее модификацию или уничтожение. Большую опасность представляют также преступные действия, связанные с доступом в информационные сети банков и иных организаций кредитно-финансовой сферы в целях совершения махинаций с финансовыми средствами.

Еще один пример махинаций такого рода — это неправомерная модификация фискальной информации контрольно-кассовых машин. Суть правонарушения в том, что организации, занимающиеся ремонтом и обслуживанием контрольно-кассовых машин по согласованию с владельцем торговой организации, где эти машины эксплуатируются, обнуляют или, иным способом, искажают имеющуюся в контрольно-кассовых машинах фискальную информацию. Часто для этого пишутся соответствующие компьютерные программы, создаются специальные программно-аппаратные комплексы, внедряемые в контрольно-кассовые машины. Таким образом от налогообложения скрываются огромные финансовые средства.

Кроме того, большое распространение в последние время получили преступления, связанные с доступом к компьютерной информации организаций-провайдеров и операторов услуг сотовой связи. В первом случае злоумышленники модифицируют информацию о работе пользователей в сети интернет и в результате получают возможность бесплатной работы в ней, нанося зачастую серьезные потери провайдеру. Как правило, для этого используются украденные пароли настоящих пользователей сети.

Доступ к компьютерной информации организаций — операторов услуг сотовой связи осуществляется с использованием специальным образом модифицированных телефонов-двойников («клонирование трубок»). В этом случае также происходит модификация информации о разговорах абонентов сети, в результате чего злоумышленник получает возможность бесплатного пользования услугами сотовой связи, нанося ущерб организации — оператору и абонентам сети.

Для совершения преступлений в сфере компьютерной информации часто недостаточно обладать определенными знаниями, необходимо иметь средства вычислительной техники и специальное программное обеспечение. Особая роль здесь принадлежит различного рода вредоносным компьютерным программам. Создание, использование и распространение таких программ составляет самостоятельный состав преступления, однако с их помощью нередко совершают другие правонарушения — неправомерный доступ к компьютерной информации, повреждение информационных систем.

Из этих программ наиболее известны компьютерные вирусы, обладающие способностью воспроизводить и распространять свои копии, а также имеющие иные функции, в том числе деструктивные. О величине возможного ущерба от компьютерных вирусов можно судить по последствиям распространения в сети интернет вируса «I love you». Так, только в Великобритании в течение одного дня вирус вызвал хаос в работе трех миллионов служащих. Работники компаний и банков получали ежедневно по электронной почте десятки писем и открывали новые послания без особого внимания. Вирус распространялся именно через электронную почту. В результате, была парализована работа банков «Барклайз», «Нэшнл Вестминстер», авиакомпании «Верджин», телекомпании «Скай нетуорк», газет «Таймс» и «Сан». Из строя были выведены многие телекоммуникационные компании. Атаке вируса подверглись также электронные сети Скотланд-ярда и парламента Великобритании. Среди других европейских стран более других от вируса пострадали Франция, Испания, Швейцария, Дания, Эстония, Норвегия и Швеция. В значительной степени были поражены также электронные сети в США, Канаде и Юго-Восточной Азии.

Терроризм и диверсии

Информация, которая играет решающую роль в функционировании структур государственной власти и национальной безопасности, общественных институтов, становится самым слабым звеном национальной

инфраструктуры государства на современном этапе развития. Глобализация современной экономики, насыщенность ее новыми информационно-телекоммуникационными технологиями, информатизация таких жизненно важных сфер деятельности общества, как телекоммуникация, энергетика, транспорт, системы хранения газа и нефти, финансовая и банковская системы, водоснабжение, оборона и национальная безопасность, структуры обеспечения устойчивой работы министерств и ведомств, переход на методы электронного управления технологическими процессами в производстве, по мнению зарубежных и российских экспертов, являются причиной все большего распространения такого явления, как кибертерроризм.

И это вовсе не надуманная угроза. Как отметил на конференции в 2000 г. в Вашингтоне по проблемам защиты от кибертеррористов Ричард Кларк, координирующий внутреннюю безопасность и защиту от террористов резиденции главы американского государства, «электронный Перл-Харбор — это не теория. Это реальность»[1]. А директор Федерального бюро расследований Луис Фри заявил в интервью программе РТР «Разговор с Америкой» о серьезности угрозы компьютерного терроризма для любой страны, где есть банковская, транспортная, энергетическая система, в особенности для страны, в которой правительство или частный сектор, как, к примеру, в США и России, опираются на информационные сети и быстрый доступ к технологиям интернет. По его словам, «отключение энергетических систем в США или электросетей в России в середине зимы, например, будет пострашнее любого теракта, с которыми мы до сих пор имели дело»[2]. Серьезную обеспокоенность по этому поводу выражают и представители российских органов государственной власти.

Под термином кибертерроризм понимаются, как правило, действия по дезорганизации автоматизированных информационных систем (АИС), создающие опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если они совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях.

Основная цель террористов состоит в том, чтобы террористический акт стал широко известен населению и органам власти, то есть получил общественный резонанс. Зачастую преступники могут не выдвигать

[1] Лента международной информации. *Интерфакс*, 20 июня 2000.
[2] Пульс планеты. *Итар-Тасс*, 21 февраля 2000.

никаких требований, анонимно действуя в целях мести, дестабилизации обстановки или устрашения. Однако особенность кибертерроризма как новой формы террористической деятельности проявляется в объективной стороне, то есть в использовании различных форм и методов временного или необратимого вывода из строя информационной инфраструктуры государства или ее элементов, а также противоправном использовании информационной инфраструктуры для создания условий, влекущих за собой тяжкие последствия для различных сторон жизнедеятельности личности, общества и государства.

В чем суть информационного терроризма?

Терроризм в качестве особой формы насилия определяется как сознательное и целенаправленное использование кем-либо насилия или угрозы насилия для принуждения политического руководства страны к реализации политических, экономических, религиозных или идеологических целей террористической организации. Важным фактором природы и мотивации терроризма является то, что террористический акт предполагает эмоциональное воздействие на общественное мнение, порождает в обществе страх, панические настроения, ведет к потере доверия к власти и в конечном итоге вызывает политическую нестабильность.

Определение понятия «информационный терроризм» достаточно трудная задача, поскольку нелегко установить четкие грани между ним, информационной войной и информационным криминалом. Другая трудность состоит в том, что необходимо выделить специфику именно этой формы терроризма.

Информационный криминал — это действия отдельных лиц или групп, направленные на взлом систем защиты, на хищение или разрушение информации в корыстных или хулиганских целях. Как сказано выше, хакеры и компьютерные воры являются типичными представителями информационного криминала. Это, как правило, разовые преступления против конкретного объекта киберпространства.

Информационный терроризм отличается от указанных форм воздействия на киберпространство прежде всего своими целями, которые остаются свойственными политическому терроризму вообще. Средства осуществления информационно-террористических действий могут варьироваться в широких пределах и включать все виды современного информационного оружия. В то же время тактика и приемы его

применения существенно отличаются от тактики информационной войны и приемов информационного криминала.

Главное в тактике информационного терроризма состоит в том, чтобы террористический акт имел опасные последствия, стал широко известен населению и получил большой общественный резонанс. Как правило, требования террористов сопровождаются угрозой повторения акта без указания конкретного объекта.

В киберпространстве могут быть использованы различные приемы достижения террористических целей, в том числе:

- нанесение ущерба отдельным физическим элементам киберпространства, например разрушение сетей электропитания, наведение помех, использование специальных программ, стимулирующих разрушение аппаратных средств, биологические и химические средства разрушения элементной базы и др.;
- кража или уничтожение информационного, программного и технического ресурсов киберпространства, имеющих общественную значимость путем преодоления систем защиты, внедрения вирусов, программных закладок и т.п.;
- воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления;
- раскрытие и угроза опубликования или опубликование закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных кодов шифрования, принципов работы систем шифрования, успешного опыта ведения информационного терроризма и др.;
- ложная угроза террористического акта в киберпространстве, влекущая за собой серьезные экономические последствия;
- захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;
- уничтожение или активное подавление линий связи, неправильное адресование, искусственная перегрузка узлов коммутации и др.;
- воздействие на операторов, разработчиков, эксплуатационщиков информационных и телекоммуникационных систем путем насилия или угрозы насилия, шантаж, подкуп, введение наркотических средств, использование нейролингвистического программирования, гипноза, средств создания иллюзий, мультимедийных средств для ввода информации в подсознание или ухудшения здоровья человека и др.

Информационный терроризм имеет в своем арсенале широкий спектр форм и методов террористической деятельности. Однако их эффективность определяется особенностями информационной инфраструктуры. К этим особенностям относятся:

- Простота и дешевизна осуществления доступа к информационной инфраструктуре. Террористические организации на правах обычных пользователей могут иметь законный доступ к инфраструктуре.
- Размытость границ информационной инфраструктуры, стирание четких географических, бюрократических, юридических и даже концептуальных границ, традиционно связанных с национальной безопасностью. Как следствие — невозможность какого-то четкого различия между внутренними и внешними источниками угроз для безопасности страны, между разными формами действий против государства (от обычной преступной деятельности до военных операций).
- Возможность манипуляции информацией и управление восприятием. Сеть интернет и ее конкуренты, которые скорее всего появятся, могут служить средством распространения пропагандистских материалов разных террористических групп для организации политической поддержки своей деятельности, дезинформации, воздействия на общественное мнение, подрыва доверия граждан к правительству.
- Недостаток информации относительно реальных и потенциальных угроз информационного терроризма, исходящих от международных и национальных неправительственных криминальных и террористических организаций.
- Необычайная сложность задач оперативного предупреждения и оценки реального или вероятного ущерба. Террористические действия могут быть проведены с беспрецедентной оперативностью. Быстрый поиск «выстрелившего ружья» будет весьма затруднен, если вообще возможен, в кризисной обстановке, в которой нет времени для осуществления правоохранительными органами традиционных следственных действий. Кроме того, не исключено, что некоторые происшествия, внешне схожие с последствиями актов информационного терроризма, будут лишь следствием неблагоприятного стечения обстоятельств.
- Трудность создания и сохранения коалиций при международном сотрудничестве. С началом серьезного информационного террористического акта, прочность коалиций государств подвергнется большому испытанию, поскольку все союзники окунутся в «информационный туман». Могут также возникнуть острые проблемы с реализацией совместных планов действий против транснациональной криминальной или террористической организации.

Для осуществления своих планов террористы могут использовать практически все типы информационного оружия.

В настоящее время имеется небольшое число мер противодействия информационному терроризму. Эти меры признаны обеспечить:

- защиту материально-технических объектов, составляющих физическую основу информационной инфраструктуры;
- нормальное и бесперебойное функционирование информационной инфраструктуры;
- защиту информации от несанкционированного доступа, искажения или уничтожения;
- сохранение качества информации (своевременности, точности, полноты и необходимой доступности);
- создание технологий обнаружения воздействий на информацию, в том числе в открытых сетях.

Экономическая и научно-техническая политика подключения государства к мировым открытым сетям должна предусматривать защиту национальных информационных сетей от информационного терроризма.

Здесь закономерна постановка вопроса о возможности совершения кибердиверсии, которая по объективным признакам схожа с терроризмом, однако в качестве цели имеет подрыв экономической безопасности и обороноспособности страны. На сегодняшней стадии проработки этих вопросов, по-видимому, нецелесообразно их дифференцировать, рассматривать отдельно друг от друга, однако необходимо иметь в виду наличие проблемы компьютерной диверсии, подпадающей под состав преступления, описанный в другой статье Уголовного кодекса.

Основной формой кибертерроризма является информационная атака на компьютерную информацию, вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, совершаемую группировками или отдельными лицами. Такая атака позволяет проникать в атакуемую систему, перехватывать управление или подавлять средства сетевого информационного обмена, осуществлять иные деструктивные воздействия.

Проникновение в сети ЭВМ, оборудованные комплексами защиты, является весьма сложной задачей, которую не всегда под силу решить самим террористам, как правило, не обладающим для этого нужными знаниями и квалификацией. Однако, располагая соответствующими финансовыми

средствами, они могут нанимать для этих целей хакеров. К тому же имеется немало программных продуктов, позволяющих значительно снизить уровень технических знаний, необходимых для информационного нападения. Для найма хакеров и приобретения соответствующих технических и программных средств не требуется слишком больших финансовых затрат. Необходимые для этого средства может выделить богатый спонсор из религиозных фундаменталистов или сторонников неофашизма.

Одной из причин такого поведения хакеров является распространенные в их среде антиобщественные настроения. Например, «Фронт освобождения интернет» ставит своей целью создание хаоса в киберпространстве исключительно из хулиганских побуждений. Но если в результате действий членов этой организации наступят тяжелые последствия, связанные, скажем, с гибелью людей, подобного рода хулиганство нельзя расценивать иначе, как террористический акт.

Опасность кибертерроризма в том, что он не имеет национальных границ и террористические акции могут осуществляться из любой точки мира. Как правило, обнаружить террориста в информационном пространстве очень сложно, так как он действует через один или несколько подставных компьютеров, что затрудняет его идентификацию и определение местонахождения.

Действия кибертеррористов могут быть направлены как на гражданские, так и на военные объекты. По мнению американских экспертов, наиболее уязвимыми точками инфраструктуры являются энергетика, телекоммуникации, авиационные диспетчерские системы, финансовые электронные системы, правительственные информационные системы, а также автоматизированные системы управления войсками и оружием. Так, в атомной энергетике изменение информации или блокирование информационных центров может повлечь за собой ядерную катастрофу или прекращение подачи электроэнергии в города и военные объекты. Искажение информации или блокирование работы информационных систем в финансовой сфере может привести к экономическому кризису, а выход из строя электронно-вычислительных систем управления войсками и оружием приведет к непредсказуемым последствиям.

Существует прямая зависимость между степенью развития информационной инфраструктуры и компьютеризации страны и количеством актов кибертерроризма. Системы спутниковой связи и глобальные сети (в первую очередь интернет) позволяют производить

атаки практически в любой точке планеты. В настоящее время проблема кибертерроризма наиболее актуальна для стран, лидирующих по этим показателям в области компьютеризации.

Так, в ноябре 1994 г. в компаниях «Дженерал Электрик» и «Нэшнл Бродкастинг Корпорэйшн» на несколько часов была нарушена работа внутренних информационных сетей. Ответственность за эту акцию взяла на себя организация «Фронт освобождения интернет», объявив «кибервойну» данным компаниям.

По сообщениям британских СМИ, в начале 1999 г. хакерам удалось захватить управление военным телекоммуникационным спутником серии «Скайнет» и изменить его орбиту. Стало известно, что специальное подразделение полиции начало расследование требований выкупа за то, что хакеры перестанут вмешиваться в управление спутником. Эти требования были предъявлены британским властям «в ряде зарубежных точек». Через несколько недель британские власти неохотно признали факт проникновения злоумышленника на запасной пункт управления спутниковой системой и незаконное вмешательство в ее работу.

До недавнего времени информационная инфраструктура Российской Федерации не представлялась сколько-нибудь уязвимой в отношении актов информационного терроризма. Причиной этого в первую очередь можно считать низкий уровень ее развития, а также значительную долю неавтоматизированных операций при осуществлении процесса управления. Вместе с тем в последние годы многие государственные и коммерческие структуры, прежде всего относящиеся к так называемым естественным монополиям, приступили к активному техническому перевооружению своих предприятий, сопровождаемому массовой компьютеризацией процессов производства и управления.

Информационная составляющая таких организаций реализуется почти исключительно на технических и программных средствах иностранного производства, что значительно повышает угрозу успешной атаки со стороны «информационных террористов». Зачастую в целях экономии средств, а также по различным субъективным причинам критически важные системы строятся без учета минимальных требований безопасности и надежности.

Информационные технологии широко используются террористическими организациями для пропаганды своей деятельности, а также вовлечения в

нее новых членов. В настоящее время в интернете находятся сайты практически всех более или менее крупных исламистских организаций, в том числе радикального толка («Международный исламский фронт», «Армия освобождения Косово», «Исламская группа» и др.). Большинство таких сайтов образуют специфическую подсеть в интернете, главные цели которой — это информационно-пропагандистское воздействие и организационная деятельность. Кроме того, интернет используется радикальными группировками в качестве средства связи. Так, по утверждению специалистов из израильской контрразведки Шин-Бет, «террористы» передают через электронную почту в зашифрованном виде инструкции, карты, схемы, пароли и т.д. Специалисты говорят о создании международной исламистской организации нового типа, основа которой не четкие организационные связи, а единая информационная среда[3].

Довольно активно возможности сети интернет используются и различного рода прочеченскими организациями экстремистского толка. По сообщениям СМИ, в ряде стран ближнего зарубежья продолжают действовать информационные центры террористов, занимающиеся тенденциозным подбором информации о ситуации на Северном Кавказе в целях манипулирования международным общественным мнением, в интернете находится ряд связанных с этим центром сайтов и размещающих подготовленную им информацию.

Сравнительно недавно был отмечен такой специфический вид кибертерроризма, как «ядерный шантаж». В начале 1999 г. через сеть интернет в адреса правительств более чем 20 стран (США, Великобритании, Израиля, Австрии и др.) были направлены электронные письма от имени офицеров-ракетчиков российской воинской части, расположенной в г. Козельске Калужской области и имеющей на вооружении стратегические ракеты шахтного базирования. В этих письмах сообщалось, что офицеры недовольны «унизительным положением России», и содержалась угроза «самовольно произвести пуски ракет по целям, расположенным в столицах и промышленных центрах западных стран». Кроме того, анонимы требовали выплаты крупной денежной суммы.

В этой связи правительства ряда стран выразили МИДу России серьезную обеспокоенность случившимся и попросили оказать содействие в розыске вымогателей. В результате проведенного ФСБ России расследования анонимы были задержаны. Ими оказались два жителя Калуги, не

[3] См.: Игнатенко А. Зеленый Internetционал. Экстремизм в компьютерной сети. *НГ-Религии*, №3/3, 7 апреля 1999.

являющиеся военнослужащими. Следствием и судом их действия были квалифицированы как сообщение о заведомо ложном акте терроризма[4].

Таким образом, угроза кибертерроризма в настоящее время является очень серьезной проблемой, причем ее актуальность будет возрастать по мере развития и распространения информационно-телекоммуникационных технологий. Поэтому правительства наиболее развитых иностранных государств принимают активные меры по противодействию проявлениям кибертерроризма.

Об осознании угрозы кибертерроризма лидерами государств, образовавшихся на постсоветском пространстве, говорит выступление на Саммите тысячелетия ООН Президента Украины Л.Д. Кучмы, указавшего на целесообразность разработки международной конвенции по борьбе с компьютерным терроризмом.

Достаточно активно этот вопрос обсуждается и в российских органах власти, в среде специалистов, а также в СМИ. Ряд ведомств высказывает пожелания дополнить существующий уголовный закон Российской Федерации отдельными статьями, предусматривающими ответственность за описанные выше деяния.

Борьба с информационными преступлениями в России
Информационная сфера уже стала сферой интересов преступного мира и в России. Как в других странах, так и в России в последние годы предметом преступных посягательств стали информация, информационная техника и технологии, информационные носители. Это обусловлено тем, что в сфере информационного бизнеса обращаются значительные денежные средства. Причем в сфере интересов криминалитета все чаще оказываются не только представители большого бизнеса, но и рядовые граждане — потребители информационных услуг.

Повышенный интерес к информационной сфере со стороны криминальных структур обусловлен:
- неуклонно растущим спросом на информационные услуги;
- высокой «рентабельностью» деятельности по осуществлению неправомерного доступа к ресурсам и услугам телекоммуникационных сетей и извлечения прибыли от их использования;
- возможностью достаточно легкого доступа к защищаемой информации через сети фиксированной и мобильных систем связи;

[4] ФСБ ру или писан ли закон взломщикам компьютеров. *Труд*, 7 июля 2000.

- наличием огромного, не использующегося по назначению, и посему дешевого интеллектуального потенциала;
- стремлением преступных сообществ к оснащению себя современными средствами связи.

Необходимость борьбы с преступностью в информационной сфере возникает там, где:
- информация, информационная техника, технологии, информационные носители выступают в качестве рыночного продукта;
- орудиями труда и средствами производства выступают информационные технологии и техника.

Особо следует выделить преступления против прав личности, защита которых гарантирована Конституцией.

При этом практическая деятельность органов безопасности в охране информационной сферы сосредоточена на борьбе с преступлениями в следующих областях:
- компьютерной техники, информатизации и телекоммуникационных сетях;
- использования информационных ресурсов;
- оборота объектов интеллектуальной собственности, реализуемых на электронных носителях;
- производства и реализации электронных систем и специальных технических средств.

Преступления в информационной сфере по неконтролируемой прибыли уверенно занимают одно из первых мест наряду с наркобизнесом и незаконной торговлей оружием.

Преступления в сфере компьютерной информации и в телекоммуникационных сетях

Компьютерные преступления носят латентный (скрытый) характер. Те из них, которые совершаются в интернете, происходят как бы в виртуальном пространстве, фактически без учета госграниц. Многие пострадавшие часто даже не подозревают, что стали жертвами злоумышленников. Часто пострадавшая сторона предпочитает не обращаться в правоохранительные органы, чтобы не навредить своей репутации. Это, прежде всего, касается крупных финансовых и государственных организаций.

Особую озабоченность вызывает распространение в глобальных информационных сетях и на электронных носителях сведений и

практических рекомендаций по подрывной деятельности и созданию оружия, включая оружие массового уничтожения (ОМУ).

Незаконный оборот объектов интеллектуальной собственности на электронных носителях

Незаконный оборот объектов интеллектуальной собственности на электронных носителях (контрафактной продукции) объективно подрывает экономические основы государства. По оценкам российских и зарубежных экспертов, оборот денежных средств составляет в этой сфере миллиарды долларов, а рентабельность преступного бизнеса — сотни процентов.

Анализ показывает что ущерб, наносимый криминалитетом затрагивает интересы как государства и правообладателей, так и рядовых потребителей реализуемой продукции. Оборот объектов интеллектуальной собственности на электронных носителях (DVD, компакт-диски с компьютерной, видео- и музыкальной информацией, аудио-, видеокассеты и др.) составляет десятки миллионов экземпляров. При этом 70-80% оборота является нелегальным, нарушающим права законных правообладателей, минует установленное налогообложение.

Незаконный оборот электронных систем и специальных технических средств

Незаконный оборот электронных систем, радиотехнических и специальных технических средств предполагает прежде всего реализацию продукции, не предназначенной для широкого использования. Это так называемые специальные технические средства, в простонародии называемые «жучки», используемые спецслужбами. Масштабы экономического ущерба в этой сфере пропорциональны общественной опасности от этих деяний.

Поток несертифицированных радио, радиотехнических и других средств наносит не только экономический ущерб. Преступников мало волнует, что использование таких средств может стать причиной нарушений в работе служб управления воздушным движением, железнодорожным, автомобильным и водным транспортом. Не разрешенные средства радиосвязи вносят помехи в каналы связи силовых структур, аварийных, спасательных и многих других служб.

Незаконный оборот электронных систем, радиотехнических и специальных технических средств по своим объемам сопоставим с

незаконным оборотом объектов интеллектуальной собственности на электронных носителях.

Неправомерный доступ к ресурсам и услугам систем связи общего пользования

В последнее время благодаря СМИ проблема неправомерного доступа к ресурсам и услугам систем связи общего пользования получила широкий общественный резонанс. По этой причине остановимся на ней более подробно.

Неправомерный доступ к конфиденциальной и коммерческой информации посредством телекоммуникационных сетей общего пользования в целях мошенничества представляет собой постоянно развивающееся и многоликое явление. Когда были введены в действие первые аналоговые мобильные сети, то обеспечение безопасности информации в них было на очень низком уровне (в частности, отсутствовало защитное кодирование как в каналах голосовой связи, так и при аутентификации абонентов), что сделало эти сети весьма уязвимыми в отношении прослушивания телефонных разговоров и клонирования телефонных трубок.

По мере перехода от аналоговых к цифровым системам (GSM) менялся и характер доступа, поскольку нарушителям становилось все труднее (и, что более важно, дороже) перехватывать информацию и «клонировать» трубки. Это привело к переходу от технического неправомерного доступа к другим видам — процедурному и контрактному. Однако полностью сбрасывать со счета возможность технического мошенничества в сетях GSM нельзя, процесс противостояния будет продолжаться.

По оценкам экспертов, из-за мошенничества отрасль мобильной связи во всем мире теряет ежегодно около 25 млрд долл., поэтому обнаружение, судебное преследование и предотвращение мошенничества так важно для всех операторов мобильной связи. Для решения этих задач в сетях необходимо принимать дополнительные меры безопасности, которые сделают их значительно менее уязвимыми с точки зрения незаконного использования ресурсов.

Однако у разных видов неправомерного доступа есть много мелких отличий, что усложняет выработку единого подхода операторов и судебных органов к анализу методов проникновения и мошенничества. Кроме того, по вопросу «Что такое мошенничество в компьютерных и телекоммуникационных системах?» вообще нет общепринятого мнения.

Определение неправомерного доступа как вида мошенничества
Упрощенно мошенничество в сетях мобильной связи можно определить как неправомочную деятельность, которая позволяет абонентам-нарушителям получать услуги связи без их установленной оплаты. Компании иногда подсчитывают деньги, которые они теряют из-за неправомерного доступа, определяя их как доходы, упущенные из-за неуплаты. Но для целей обнаружения факта преступления от такого определения мало пользы, поскольку исходя из него, мошенничество можно обнаружить только постфактум. Дать точное определение того, что есть мошенничество, может быть и невозможно, так как на практике различие между мошенническим и правомочным (не мошенническим) поведением бывает бесконечно мало. Тем не менее, мы попробуем определить, что такое неправомерный доступ исходя из примеров мошеннического поведения.

Классификация неправомерного доступа
Поскольку мошенничества могут происходить во всем спектре услуг и применений систем связи, то рассмотрение отдельных примеров или ситуаций непродуктивно. Поэтому, чтобы структурировать эту проблему и сделать ее более понятной, выделим четыре основных вида неправомерного доступа в телекоммуникационных сетях.

Контрактный доступ. Мошенничества с использованием контракта весьма многообразны, но все ситуации можно разделить на две категории. Первая — когда контракт заключается без намерения оплачивать услуги, или — когда абоненты, заключающие контракт, принимают решение не оплачивать услуги в какой-то момент после начала действия контракта.

Вторая категория — мошенничество при использовании льготного тарифа, в том числе включает получение некоторой службой права пользования льготным тарифом и приобретение абонентом-нарушителем (или группой таких абонентов) нескольких номеров телефонов, для того чтобы звонить по номеру этой службы. В зависимости от схемы оплаты службы с льготным тарифом видоизменяются механизм мошенничества и его отличительные признаки.

Фрикерский доступ. Все виды мошенничества этой категории дают доход мошеннику за счет проникновения в незащищенную систему и использования (либо последующей продажи) имеющихся в системе функциональных возможностей. Примерами являются использование в целях мошенничества Московской городской телефонной сети (местной

автоматической телефонной станции (АТС)) и фрикерское нападение на сеть (фрикерская атака или взлом сети).

В случае фрикерства в АТС мошенник многократно звонит в АТС, стараясь получить доступ к внешней исходящей линии. Получив такой доступ, он затем может вести дорогостоящие телефонные разговоры, оплатив только недорогой звонок за доступ к АТС. Зачастую такие звонки увязаны с использованием клонированных телефонов, так что не оплачивается даже использование недорогой местной линии.

Технический доступ. Все виды проникновения этой категории включают атаки на слабые технологические участки мобильной системы. Обычно для такого мошенничества требуется наличие у нарушителей некоторых начальных технических знаний и способностей, хотя после обнаружения слабых мест системы информация о них зачастую быстро распространяется в форме, понятной и для технически необразованных людей. Примерами такого мошенничества являются клонирование трубок и внутри корпоративное техническое мошенничество.

При клонировании параметры аутентификации мобильного телефона копируются в другой мобильный телефон, а оператор сети полагает, что работает исходный телефон, который ранее был аутентифицирован. При внутрикорпоративном техническом доступе сотрудники компании (нарушители) могут внести изменения в определенную внутреннюю информацию, чтобы получить доступ к услугам по сниженной стоимости.

При атаке на АТС используется аппаратура подмены абонентского номера. На запрос АТС посылается встречный импульс с заведомо ложной информацией, обеспечивающей свободный автоматический (разрешенный как услуга сети) выход на междугородную, международную связь. Открывается доступ, и мошенник звонит и разговаривает круглые сутки.

Процедурный доступ. Все виды проникновения этой категории включают атаки на процедурные алгоритмы, предназначенные для уменьшения риска мошенничества, и часто направлены на слабо защищенные места биллинговой системы, бизнес-процедур, используемых для предоставления доступа в систему.

Примерами таких видов воздействия являются неправомочное использование режимов роуминга, дублирование идентификаторов телефонных карт (смарт-карт) и использование фальшивых телефонных карт.

Исходя из реальных оперативно-технических возможностей на сегодняшний день, выявляется всего несколько процентов действующих радиотелефонов-«двойников», переговорных пунктов и случаев несанкционированного подключения к сетям телефонной связи. При этом несовершенство правовой базы не позволяет зачастую принимать адекватные меры к нарушителям, бороться с преступностью в этой сфере. Позволим себе повториться, данный криминальный бизнес по уровню рентабельности вышел на лидирующие позиции.

Неуклонно возрастает и степень опасности данного вида преступности для общества и государства. Одна из главных задач преступных сообществ в этом направлении — получение негласного доступа к системам радио- и радиотелефонной связи общего и государственного назначения с целью получения конфиденциальной и служебной информации для использования ее в преступных целях. В последнее время у организованных преступных групп становится популярным использование радиотелефонов-«двойников» при совершении преступлений, связанных с похищением людей, вымогательством, угрозой насилием или физического уничтожения, совершением мошеннических действий через подставные фирмы и др., т.е. в тех случаях, когда преступники имеют надежную постоянную телефонную связь как между собой, так и с объектом преступного посягательства, а местоположение их определить очень сложно.

Информационная безопасность бизнеса

Любая деятельность строится на основе информации. Информация является системообразующей составляющей любой организации. Но особое значение информация имеет для современного бизнеса. От качества информации, от того насколько она адекватна по содержанию и форме представления потребностям пользователей, насколько она полна и достоверна, насколько она точна и конкретна, насколько вовремя она поступает, во многом зависит конкурентоспособность фирмы, эффективность ее функционирования и управления ею и, в конечном счете, ее жизнеспособность.

Кроме того, деятельность фирмы, а значит, и ее судьба, становятся, все в большей степени, зависимы от надежности и защищенности компьютерных систем, на основе которых реализованы ее информационные системы. Нарушение в функционировании АИС может

повлечь за собой существенные проблемы в функционировании фирмы, сказаться на ее конкурентоспособности, а в некоторых, наиболее серьезных случаях, повлечь и прекращение ее деятельности.

Новые формы бизнеса с применением информационных технологий
На начальных этапах внедрения информационных технологий в деятельность организаций они использовались главным образом в системах учета и контроля. В настоящее время АИС все активнее используются в качестве ядра бизнес-процессов. Компьютеры стали основным инструментом управленческого персонала. Все шире используются информационные технологии для обслуживания клиентов. Сейчас невозможно найти банк, в котором бы обслуживание клиентов велось без компьютерной сети.

Новый импульс для использования информационных технологий в бизнесе дал интернет. Сначала его роль сводилась главным образом к роли нового канала коммуникаций — через электронную почту пошел основной поток переписки между сотрудниками фирм. В настоящее время наиболее популярными являются два направления развития бизнеса через интернет получивших названия: «business to business» (B2B) и «business to customer» (B2C).

Первое направление, B2B, предполагает построение систем, обеспечивающих ведение бизнеса с использованием интернет при работе с корпоративными клиентами.

Второе направление, B2C, предполагает использование систем, предназначенных для обслуживания с помощью интернет клиентов-частных лиц.

B2B включает в себя такие виды бизнеса, как:
- электронные биржи;
- системы оптовой торговли через интернет;
- системы работы с дилерами и дистрибьюторами.

B2C включают:
- электронные магазины, торгующие всевозможными товарами широкого потребления;
- системы торговли валютой и финансовыми инструментами;
- системы бронирования и заказов всевозможных услуг.

Можно выделить два основных пути становления новых форм бизнеса с применением интернет. По первому идут организации, занимающиеся традиционным бизнесом, которые пытаются с помощью интернет найти новых покупателей, усовершенствовать работу с поставщиками, подрядчиками, клиентами или открыть для себя новое поле деятельности. Через интернет оформляются заказы, производятся расчеты, осуществляется техническая поддержка пользователей и потребителей.

Частным случаем развития подобных тенденций является создание систем биржевой торговли через интернет. В результате создано множество биржевых интернет-площадок для торговли сырьевыми товарами, валютой и ценными бумагами.

Другим направлением становления интернет-бизнеса является развитие его компаниями, которые начинали свою деятельность с создания информационных технологий и средств информатизации. Разработав программное обеспечение, позволяющее вести торговлю через интернет, такого рода фирмы находят партнеров, занимающихся традиционным бизнесом, или выпускают акции. Получив оборотный капитал, они создают собственные склады с товарами, заключают договоры с фирмами, осуществляющими доставку товаров и с платежными системами, специализирующимися на проведении расчетов через интернет, и начинают торговлю.

Говоря об интернет-бизнесе, помимо B2B и B2C нельзя не упомянуть и такие, на сегодняшний день ставшие уже традиционными, виды деятельности в интернете, как интернет-реклама, информационные услуги и поставка контента для информационных сайтов.

Интернет-рекламой занимаются специализированные рекламные агентства, которые изготавливают и размещают баннеры на наиболее популярных интернет-порталах, вэб-страницах, в системах баннерного обмена.

Специальные информационные серверы, поисковые системы и порталы зарабатывают в основном за счет размещения на их страницах рекламных баннеров. Из поступающих доходов они оплачивают услуги организаций-поставщиков информационного контента. Еще одним источником доходов информационных серверов являются платные информационные услуги, предоставляемые, как правило, по подписке, создание магазинов электронной торговли, или оказания качественно новых информационных услуг, таких как голосовая почта.

Ну и, наконец, в качестве не самых больших, но зато, возможно, самых важных для будущего развития интернет-бизнеса, необходимо упомянуть сектора платежных систем и систем поддержки электронного документооборота.

Платежные системы призваны обеспечивать осуществление платежей в интернете. Их доход складывается из комиссионных от проведенных операций. От успеха развития этих организаций во многом зависит судьба большого числа интернет-магазинов, рост их клиентуры и объемов продаж, развитие дистрибьютерских сетей в регионах. Но еще в большей степени в зависимости от их популярности и успешности находится развитие индустрии оказания всевозможных платных информационных услуг через интернет.

Организации, выполняющие функции систем поддержки электронного документооборота, обеспечивают выдачу и подтверждение сертификатов криптографических ключей. Роль такого рода организаций, в качестве доверенных посредников, при осуществлении сделок через интернет, а также их число, вероятно, будут возрастать по мере расширения использования интернета в бизнесе, расширения и укрепления нормативной и законодательной базы интернет-экономики. Основным источником доходов такого рода компаний является плата за выдаваемые ими сертификаты криптографических ключей.

Отечественный сектор фирм, занимающихся интернет-бизнесом, пока очень слаб. В России развитию новых форм бизнеса с применением интернета в значительной степени препятствует отсутствие достаточно надежной нормативно-правовой и законодательной базы, а также отечественных систем поддержки электронного документооборота и электронных платежей. Кроме того, мешает отсутствие непротиворечивой нормативно-правовой базы по вопросам применения криптографии. И если в законодательной области в ближайшее время можно рассчитывать на какие-то сдвиги, в связи с ожидаемым принятия закона о цифровой подписи, то в области криптографического обеспечения интернет-бизнеса ситуация остается без изменения.

С одной стороны, на сегодняшний день легальным является использование только сертифицированных средств криптографической защиты информации. С другой стороны, предлагаемые отечественными структурами сертифицированные средства и системы криптографической защиты ориентированны сугубо на внутрикорпоративные решения или

предназначены для создания систем обслуживания узкого круга клиентов и не применимы для реализации реальных крупномасштабных интернет-проектов. В результате, на сегодняшний же день можно зафиксировать тот факт, что даже самые популярные отечественные платежные системы, такие как Assist, Webmoney и Cyberplat, реализованы на основе зарубежных или собственных несертифицированных криптографических средств, что делает их весьма уязвимыми как с точки зрения отечественного законодательства, так и с точки зрения гарантий их безопасности.

В ближайшее время в России ожидается принятие закона «Об электронной цифровой подписи». Подготовлены и обсуждаются проекты законов «Об электронном документе» и «О предоставлении электронных финансовых услуг». Можно ожидать, что с учетом типового закона ЮНСИТРАЛ (UNCITRAL — United Nations Commission on International Trade Law, Комиссия ООН по праву международной торговли) об электронной коммерции будет принят соответствующий закон в России. Таким образом, будут обеспечены все условия для развития бизнеса на основе современных информационных технологий.

Традиционные и новые угрозы и методы обеспечения информационной безопасности бизнеса

Угрозами информационной безопасности бизнеса в «докомпьютерную» эпоху были:

- промышленный и экономический шпионаж;
- утрата документации в результате хищений, пожаров или стихийных бедствий;
- недобросовестность, некомпетентность или злой умысел сотрудников.

Традиционные системы хранения документации в одном месте на бумаге делали безвозвратными потери информации в случае пожара или других катастрофических событий и очень часто приводили к тому, что организации не могли продолжать свою деятельность после таких случаев. Некомпетентность, недобросовестность, небрежность или злой умысел сотрудников мог приводить к потере документов, искажению информации (приписками), к ошибкам в отчетности.

Организации, занимающиеся бизнесом, обречены на развитие своих информационных систем, поскольку без их развития невозможно развитие самого бизнеса. С внедрением АИС, для предотвращения хищений информации, появляется возможность ее шифрования, разграничения доступа для различных категорий персонала. Для того чтобы обеспечить

невозможность уничтожения информации в результате тех или иных катастрофических событий или хищений, появилась возможность распределенного резервного хранения копий этой информации в нескольких территориально разнесенных между собой местах (на электронных носителях или в отдельных узлах территориально-распределенных сетей). Появились хорошие системы логического контроля информации, снизившие возможности приписок и ошибок со стороны сотрудников. Однако применение АИС несет с собой множество новых угроз и рисков нарушения информационной безопасности. Чем более функциональной и, соответственно, более сложной является АИС, используемая в организации, тем более она уязвима и тем больше внимания должно быть уделено ее защите.

Для обеспечения безопасности создаваемой АИС необходимо соблюдать целый ряд правил:

- поручать создание подсистем информационной безопасности, а по возможности и всей АИС, организациям, имеющим лицензии специальных органов, осуществляющих надзор за безопасностью информационных систем;
- отдавать предпочтение средствам информатизации сертифицированным специальными органами, осуществляющими надзор за безопасностью средств информатизации;
- проводить оценку предлагаемых проектных решений и средств информатизации с точки зрения безопасности информационных технологий;
- проводить анализ угроз и оценку рисков, связанных с реализацией предлагаемых проектных решений, с целью определения достаточности закладываемых решений по защите АИС;
- выработать и исполнять политику безопасности, в том числе в форме соответствующих нормативных документов;
- обеспечить внедрение средств защиты АИС от несанкционированного доступа.

На этапе эксплуатации АИС для обеспечения информационной безопасности бизнеса должна быть создана полноценная система управления информационной безопасностью. В рамках этой системы должны решаться следующие задачи:

- контроль и управление функционированием подсистемы информационной безопасности;
- непрерывный мониторинг защищенности АИС и регистрация попыток вторжения;
- разбор и расследование фактов нарушения информационной безопасности;

- изучение известных моделей хакерских атак и взлома компьютерных систем, анализ возможностей их реализации в отношении АИС фирмы, принятие мер по устранению возможностей реализации такого рода атак и методов взлома;
- организация антивирусной защиты компьютеров организации;
- мониторинг возможных угроз нарушения информационной безопасности;
- управление рисками нарушения информационной безопасности и их страхование;
- управление персоналом, в аспектах, связанных с обеспечением информационной безопасности организации.

Одним из наиболее важных направлений в управлении информационной безопасностью бизнеса является анализ угроз нарушения информационной безопасности и выработка мер по их отражению или снижению ущерба в случае их возможной реализации.

Все угрозы информационной безопасности бизнеса можно разделить на следующие виды:
- угрозы утечки информации по каналам, не связанным с использованием АИС;
- угрозы несанкционированного доступа к ресурсам АИС без использования телекоммункационного доступа;
- угрозы несанкционированного доступа через телекоммуникационные сети;
- угрозы системам электронного документооборота и платежным системам;
- угрозы информационной безопасности, не связанные с несанкционированным доступом к информации.

При анализе опасности угроз принято брать в расчет то, как они влияют на доступность, конфиденциальность и целостность информации.

Очевидно, что руководство фирмы должно каждый раз само решать, какие угрозы являются первоочередными и какие меры противодействия нужно использовать. Для этого оно должно проанализировать риски и угрозы, выявить среди них наиболее опасные и принять те меры, которые помогут их существенно снизить.

Для больших гарантий защиты бизнеса все чаще прибегают к финансовому страхованию рисков нарушения информационной безопасности организации.

Что касается России, то, как было показано выше, в значительной степени условия информационной безопасности бизнеса здесь зависят не только от конкретных организации, где эта безопасность должна обеспечиваться, но и от множества внешних факторов, а также решения общих для страны проблем. Естественно, в решении такого рода проблем особая роль принадлежит государству. О том, что это достаточно глубоко осознано руководством страны, можно судить по «Доктрине информационной безопасности Российской Федерации». Этот документ содержит постановку практически всего спектра задач, которые должны быть решены для обеспечения нормальных условий развития бизнеса в масштабе всей страны с точки зрения обеспечения его информационной безопасности. Вопрос только в принятии конкретных решений и выполнении действий, направленных на достижение поставленных целей.

Безопасность открытых информационных сетей

Практические приложения проблемы информационной безопасности так или иначе связаны с передачей информации и информационным обменом, что в современных условиях не может обеспечиваться иначе как через использование информационных и информационно-телекоммуникационных сетей. И если вопрос безопасности закрытых сетей с успехом может решаться за счет технических и организационных возможностей организаций, их эксплуатируемых, то в отношении открытых сетей, а их становится и будет все больше, коль скоро мы стремимся к единому общедоступному информационному пространству, обеспечение безопасности их работы и работы с ними становится все более сложной проблемой. Мало того, она не редко становится узловой при решении других задач информационной безопасности.

Что же такое открытые информационные сети (ОИС) и в чем их отличие от других, закрытых информационных сетей, например, информационной сети какого-либо ведомства или организации?

Первое — эти сети общедоступны, то есть их использование не требует принадлежности пользователя к какому-либо специализированному сообществу.

Второе — ОИС обеспечивают информационное взаимодействие с другими ОИС.

Третье — ОИС обеспечивают информационный обмен без каких-либо ограничений и внесения искажений в передаваемую информацию.

Четвертое — ОИС используют единую, согласованную систему протоколов обмена и форматов представления информации, обеспечивающую информационный обмен по сети различными видами информации (текст, звук, изображение и т.д.).

Отдельные ОИС, как правило, объединяются в разветвленную сеть информационного обмена и доступа к открытым для общества информационным ресурсам. Можно говорить о том, что «всемирная паутина» интернета — это конгломерат взаимодействующих по заранее оговоренным правилам ОИС различных стран и организаций, которые обеспечивают, практически без ограничений, информационные взаимодействия между любыми пользователями каждой из ОИС.

Как и любое другое достижение научно-технического прогресса, развитие ОИС наряду с положительными имеет и отрицательные последствия. Одним из таких отрицательных последствий является существенное возрастание опасности реализации угроз информационной безопасности тех объектов и информационных ресурсов, которые подключены к ОИС. Получается парадокс — чем большее количество пользователей страны включается в ОИС и чем выше положительное воздействие этого процесса на общее социально-экономическое и политико-культурное развитие государства и общества, тем более значимой становится проблема обеспечения информационной безопасности страны. Это относится как к обеспечению информационной безопасности государственных и коммерческих объектов, так и безопасности общества и информационных прав граждан, конфиденциальности личной информации. Соответственно, обеспечение информационной безопасности ОИС должно предусматривать защиту от внутренних и внешних угроз ее нарушения.

Исходя из сказанного, основная задача обеспечения информационной безопасности в ОИС может быть сформулирована как гарантированно высокое обеспечение пользователю целостности, достоверности, доступности и конфиденциальности циркулирующей в сети информации, а также информационных ресурсов, использующих данную сеть пользователей при воздействии на ОИС любого набора внешних и внутренних угроз нарушения информационной безопасности.

Первый класс особенностей ОИС с точки зрения информационной безопасности заключаются в том, что нарушения целостности, достоверности, доступности и конфиденциальности циркулирующей в сети информации может быть произведено двояко: это может быть проделано в самой сети путем противоправного проникновения в нее или организации «утечки информации»; это может быть выполнено путем проникновения с помощью сети в компьютер (компьютерную сеть) пользователя.

В первом случае ставится задача защиты самой ОИС от реализации возможных угроз ее разрушения и/или нарушения целостности. Во втором — защиты интерфейсов сеть-пользователь от возможности несанкционированного проникновения из сети в систему пользователя. Очевидно, что набор угроз нарушения ИБ и средств их парирования в каждом варианте несколько различен.

Второй класс особенностей ОИС с точки зрения информационной безопасности связан с глобальным характером ОИС, что определяет возможность реализации любой угрозы извне, из-за пределов данной страны. Это означает, что сегодня уже невозможно обеспечить информационную безопасность сети только в пределах данной страны и возникает необходимость разработки международных правил и регуляций, определяющих условия обеспечения информационной безопасности в рамках всей глобальной сети.

Сегодня уже мало кому надо объяснять опасность нарушения информационной безопасности в ОИС. Необходимо открыто говорить о том, что случаи информационного криминала начинают приобретать массовый характер и требуют эффективного использования пользователями, в особенности участниками финансово-торговой деятельности, всех известных методов и средств обеспечения информационной безопасности в ОИС.

В информационных войнах и противоборстве глобальные ОИС могут широко использоваться в качестве основного средства внедрения информационного оружия в национальную информационно-коммуникационную инфраструктуру противника для ее разрушения и вывода из строя его систем управления.

В настоящее время национальные инфраструктуры ОИС не обеспечивают гарантированной защиты информации пользователей. Информация, получаемая из интернета или отправляемая через интернет, может быть искажена, сфабрикована, вскрыта, прочитана и распространена без

ведома авторов. В результате интернет может стать глобальным механизмом дезинформации, компрометации и махинаций. Бесконтрольное использование шифровальных средств может сделать интернет идеальной средой обмена криминальной информацией.

Нужно сделать так, чтобы среда гарантированно-защищенного обмена информацией была доступна для всех законопослушных пользователей ОИС. Создание такой среды откроет самые широкие возможности по развитию предпринимательства, электронной коммерции, телемедицины, электронного правительства, других социальных институтов, сделает возможным авторизованный доступ к любой информации, переведенной в электронную форму, снизит расходы на защиту информации для всех организаций и фирм, избавит их от необходимости внедрять собственные дорогостоящие системы защиты телекоммуникационного обмена информацией.

Однако создание такой среды возможно только путем развития инфраструктуры защиты информации в открытых сетях. В мире накоплен большой опыт создания инфраструктур защиты информации. Хотя нельзя сказать, что где-то уже создана идеальная инфраструктура защиты информации в открытых сетях, но движение в этом направлении в развитых странах можно отследить практически повсеместно.

Создание инфраструктуры защиты информации в открытых сетях предполагает, что пользователи открытых сетей должны иметь возможность использовать стандартные гарантированно-надежные криптографические алгоритмы. Соответственно, должна существовать инфраструктура, обеспечивающая гарантии безопасности пользователям систем шифрования, а также интересы государства по обеспечению информационной безопасности в ОИС.

В целом можно говорить о том, что в настоящее время в России и в других странах еще не осознана необходимость комплексного системного подхода к решению проблем обеспечения информационной безопасности в открытых сетях. Пока еще делаются попытки временного «латания» проявляющихся «узких мест» и всевозможных «дыр» в эксплуатируемых и создаваемых информационных системах, входящих в открытые компьютерные сети. Однако такого рода решения могут дать только временный эффект — тут же появляется новая «дыра», которую также необходимо срочно заделывать, и т.д., и т.п. Данный процесс обычно становится перманентным и не обеспечивающим гарантированную защиту информации пользователя открытой сети.

Значимость задачи обеспечения информационной безопасности в глобальной инфраструктуре открытых сетей связана с двумя особенностями ОИС. Во-первых, все эти сети имеют глобальный характер, но не имеют организующего их функционирование органа, который мог бы отвечать или принимать меры по обеспечению в них информационной безопасности. Соответственно, отсутствует единая правовая база регулирования развития и происходящих в сетях процессов (вне зависимости от того, положительные эти процессы или негативные). Во-вторых, информационный обмен имеет, в большинстве случаев, трансграничный характер, связывая между собой корреспондентов, деятельность которых регулируется различными, принятыми в данной стране правовыми положениями. Очевидно то, что приемлемо во Франции или Нидерландах, может быть совершенно неприемлемо в Иране или Китае.

Соответственно, возникает задача обеспечения информационной безопасности международного информационного обмена во всех его сферах, осуществляемого по глобальным ОИС. Данную задачу также следует рассматривать системно, т.е. учитывая такие факторы, как неравномерность информационного, экономического и политического развития различных стран, наличие или отсутствие соответствующего законодательства в стране, степень участия в международной деятельности по решению данной проблемы. Такое рассмотрение связано с тем, что именно глобальные ОИС являются наиболее уязвимым (с точки зрения обеспечения информационной безопасности) элементом всей системы международного информационного обмена.

Таким образом, говоря в целом о проблеме информационной безопасности в ОИС, можно констатировать следующее:

1. Комплекс проблем обеспечения информационной безопасности представляет собой классический пример сложной задачи, требующей системного решения. Попытки решения этой задачи «по частям» не дают и не могут дать удовлетворяющего общество результата. Это относится как к проблемам обеспечения информационной безопасности национальной инфраструктуры ОИС, так и обеспечению информационной безопасности глобальной системы ОИС.
2. В рамках страны задача может быть решена только в случае формирования общенациональной среды гарантированно-защищенного обмена информацией. Однако создание такой среды возможно только путем развития инфраструктуры защиты информации в открытых сетях.
3. Решение проблем обеспечения информационной безопасности глобальной системы ОИС может быть обеспечено лишь при тесном

взаимодействии всех стран при выработке основополагающих и взаимоприемлемых положений и правил, регулирующих процессы международного информационного обмена.

4. Необходимо осознание всем мировым сообществом, властными структурами и общественностью стран важности, значимости, сложности и жесткой необходимости совместного решения этой жизненно важной проблемы — обеспечения информационной безопасности ОИС.

Информационно-психологическая безопасность

В Доктрине информационной безопасности Российской Федерации введено понятие «противоправные информационно-психологические воздействия». Такие воздействия рассматриваются в Доктрине как серьезные угрозы личности, обществу и государству и, прежде всего, конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию.

Речь идет о возможных деформациях системы массового информирования и распространении дезинформации, ведущих к потенциальным нарушениям общественной стабильности, о нанесении вреда здоровью и жизни граждан, вследствие пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду, о деятельности тоталитарных сект, пропагандирующих насилие и жестокость. Эти воздействия, осознаваемые или неосознаваемые, как показывает жизнь, могут приводить и в действительности приводят к серьезным нарушениям психического и физического здоровья, размыванию естественных и культурно-заданных норм поведения, к росту рискованных социальных и личностных ситуаций.

В настоящее время влияние новых источников и технологий информационно-психологические воздействия на общество в целом, на организованные группы, неорганизованные массы людей и на отдельного человека непрерывно растет.

Информационно-психологические воздействия как угрозы безопасности личности, общества и государства

Есть несколько планов описания и анализа информационно-психологических воздействий. Первый и второй планы относятся собственно к индивиду (личности).

Первый рассматривает человека как субъект политической жизни, носителя определенного мировоззрения, обладающего более или менее выраженными правосознанием и менталитетом, духовными идеалами и ценностными установками. Гражданин есть сознательный субъект отношений с обществом и властью (государством) и он строит свое поведение в том числе в зависимости от того, насколько он этой власти доверяет. В этом контексте формирование доверия к себе есть одна из основных политических задач власти. Неадекватное общественным (с точки зрения власти) интересам поведение гражданина может принимать как острые формы политического экстремизма, угрожающие самому существованию политической системы, так и политического равнодушия, в не меньшей степени подрывающего основы общественной жизни.

Второй план рассматривает человека как индивида, обладающего сознанием, подверженным различного рода манипулятивным воздействиям, информационным по своей природе, результаты которых могут прямо угрожать физическому или психическому здоровью человека. Именно такие воздействия часто на протяжении многих лет формируют морально-психологическую атмосферу в отдельных слоях общества, питают криминальную среду и способствуют росту психических заболеваний в обществе. Сектантское проповедничество, распространение мистических и эзотерических учений и практик, магии, шаманства и т.п. могут служить примером таких воздействий, приводящих к социальной и личностной дезадаптации, а в ряде случаев к разрушению психики человека.

Серьезную опасность для психики вызывает распространение по сети интернет прежде всего порнографии, непристойной и оскорбляющей общественную нравственность информации, нарушающее сложившиеся в обществе стандарты морали. Серверы с такой информацией часто посещаются детьми и подростками. Ведь посредством интернета гарантируется куда большая конфиденциальность и анонимность, чем посещение кинотеатров или магазинов с открытой или подпольной порнолитературой и порновидеофильмами.

Информационно-психологические воздействия на массовое сознание. Третий план предусматривает анализ информационных воздействий на организованные или неорганизованные (толпа) группы и массы людей. Цель этих воздействий — вызвать особое, конфликтное поведение в острых жизненных (политических, военных, чрезвычайных) ситуациях. Инициация паники, принуждение к сдаче в плен, мобилизация митингующих к активным действиям — вот несколько примеров таких целей. Тонкие

механизмы их реализации, использующие свойства массового сознания, описаны в известной литературе по психологической войне.

Четвертый план ставит проблему информационно-психологического воздействия на население страны в целом или в региональном масштабе. Речь идет о наиболее подверженной манипулятивным воздействиям маргинальной части населения, к которой принадлежат прежде всего социально-незащищенные граждане. Именно на них информационно-психологическое воздействие оказывает сильное моральное и психологическое давление, ложащееся на общий фон бедности и неустроенности в жизни. Можно говорить о морально-психологических последствиях информационно-психологического воздействия на население страны, степень тяжести которых существенно зависит от господствующих в массовом сознании стереотипов восприятия и оценки условий социальной жизни. Эта оценка, впрочем, практически полностью формируется непрерывным потоком информационно-психологического воздействия, обрушивающимся на головы людей.

Информационно-психологические воздействия — негативный контекст. Когда говорят об информационно-психологическом воздействии как угрозах, естественно, подразумевают негативные последствия их реализации. Однако вопрос о негативности заслуживает специального рассмотрения. Представляется справедливым такое определение: «Негативные информационно-психологические воздействия — это, прежде всего, манипулятивные воздействия на личность, на ее представления и эмоционально-волевую сферу, на групповое и массовое сознание, инструмент психологического давления с целью явного или скрытого побуждения индивидуальных и социальных субъектов к действиям в ущерб собственным интересам в интересах отдельных лиц, групп или организаций, осуществляющих эти воздействия»[5].

Здесь требуется пояснение, поскольку есть один тонкий момент, обусловленный самим фактом манипуляции — ведь в исходном смысле этого термина заложен негативный, провокативный контекст. Отдельные виды информационно-психологического воздействия, обращенные к населению в целом или адресованные конкретным лицам, социальным слоям и группам, политическим партиям и движениям, способны серьезно нарушить нормальное функционирование и жизнедеятельность социальных

[5] Аносов В.Д., Лепский В.Е. Исходные посылки проблематики информационно-психологической безопасности. В книге: Брушлинский А.В., Лепский В.Е. (ред.). Проблемы информационно-психологической безопасности. М., ИП РАН, 1996, с.7-11.

институтов, государственных структур, общественных организаций, объединений граждан и отдельных лиц. Эти воздействия квалифицируются именно как негативные, так как вызывают психоэмоциональную и социально-психологическую напряженность, искажение нравственных критериев и норм, морально-политическую дезориентацию и, как следствие, неадекватное поведение отдельных лиц, групп и масс людей.

Но государство, власть как политический институт вообще, также прибегает к манипуляции сознанием людей. Все дело в политических критериях направленности манипулятивных воздействий. Максимально независимый от конкретной политической позиции (левые, правые, центр, экстремальные позиции) политический критерий негативности можно сформулировать следующим образом[6]:

Демократическое государство — гарант социальных прав и свобод граждан и инструмент сдерживания возможных деструктивных результатов воздействий корпоративных и личных интересов. Именно из этого идеала следует исходить. Если информационно-психологические воздействия работают против таких функций и деятельности, то такие воздействия следует квалифицировать как негативные, как угрозы индивидуальному и массовому сознанию, что присуще, как правило, авторитарным и тоталитарным режимам.

Индивидуальное и массовое сознание как объекты информационно-психологические воздействия

Индивидуальное сознание. Для личности главными системообразующими качествами являются целостность (тенденция к устойчивости) и развитие (тенденция к изменению). При разрушении или искажении этих качеств личность перестает существовать как социальный субъект. Это означает, что любые информационно-психологические воздействия на личность должны оцениваться с позиций сохранения или разрушения ее как целого.

Информационно-психологические воздействия на индивидуальное сознание могут привести к двум видам взаимосвязанных изменений.

Во-первых, это изменения психики, психического здоровья человека. Поскольку в случае информационных воздействий трудно говорить о границах нормы и патологии, показателем изменений могут служить потеря адекватности отражения мира в сознании и своего отношения к

[6] См., например: Шерковин Ю.А. Психологические проблемы массовых информационных процессов. М., Мысль, 1973; Шиллер Г. Манипуляторы сознанием. Пер. с англ. М., Мысль, 1980.

миру. Можно говорить о деградации личности, если формы отражения действительности упрощаются, реакции огрубляются и осуществляется переход от высших потребностей (в самоактуализации, социальном признании) к низшим (физиологическим, бытовым).

Во-вторых, это сдвиги в ценностях, жизненных позициях, ориентирах, мировоззрении личности. Такие изменения влекут за собой антисоциальные поступки и представляют опасность уже для всего общества и государства.

Важная особенность информационно-психологических воздействий на индивидуальное сознание состоит в том, что они как угрозы могут не замечаться и не осознаваться самим человеком.

Массовое сознание. Известны социально-психологические особенности массового сознания: доверчивость к печатному слову, теле- и радиоинформации на государственных и негосударственных каналах СМИ, готовность к восприятию политических и квазинаучных мифологем. Массовое сознание формируется прежде всего жизненным опытом и уж затем вследствие информационных воздействий. Тем не менее, информационно-психологические воздействия могут существенно изменять массовое сознание и поведение больших групп населения (социумов).

По отношению к информационным процессам массы могут рассматриваться в трех формах: как население, толпа или коллектив. Основными источниками информации, влияющими на сознание населения, являются СМИ и слухи. Для толпы главный источник информации — лидер и его ближайшее окружение (харизматическое ядро), а также слухи и особо экзальтированные лица в самой толпе. В коллективе ведущее значение имеет официальная информация, поступающая от должностных лиц, и сообщения неформального лидера.

Особой специфики в воздействии информации на массы, находящиеся в нормальном (т.е. спокойном, уверенном) психологическом состоянии, нет. Гораздо меньше известно об особенностях информационно-психологического воздействия на массы, находящиеся в состояниях, отличающихся от нормального, т.е. характерных для рискованных социально-психологических ситуаций.

Под рискованными социально-психологическими ситуациями понимаются такие состояния и действия масс, которые с большой вероятностью могут привести или фактически приводят к нарушению

нравственных или правовых норм, и в результате этого являются опасными для нормальной жизнедеятельности социума[7].

Динамику зарождения и развития рискованных социально-психологических ситуаций можно представить в виде следующей схемы: Первая стадия — «брожение масс», недовольство ситуацией, выявление общих (объединяющих) потребностей, осознание и принятие большинством общей цели и единого мнения о наличии внешних угроз.

Вторая стадия — осознание того, что и когда нужно делать для удовлетворения общих потребностей и преодоления препятствия или устранения угрозы, формирование ролевой коллективной (групповой) структуры и общего эмоционального настроя на борьбу.

Третья стадия — активные действия по достижению цели с использованием легитимных информационно-психологических способов воздействия на противостоящую сторону.

Четвертая стадия — активные действия с использованием нелегитимных способов воздействия вплоть до силовой борьбы.

Пятая стадия — (в случае недостижения цели) — спад настроения или возникновение паники, прекращение активных действий, переосмысливание программы действий и, возможно, перестройка ролевой структуры социума.

Источники, каналы распространения и технологии информационно-психологического воздействия

В этом разделе рассматриваются различные инструменты информационно-психологического воздействия, преимущественно, в технологическом аспекте. Традиционные механизмы пропагандистского манипулирования массовым сознанием остаются за рамками настоящей работы.

Для реализации информационно-психологического воздействия на индивидуальное, групповое и массовое сознание используются следующие источники, каналы распространения и технологии (средства):

- средства массовой информации и специальные средства информационно-пропагандистской направленности;
- глобальные компьютерные сети и программные средства быстрого распространения в сети пропагандистских информационных материалов;

[7] Зараковский Г.М., Авдеева Н.Н., Степанова Г.Б. Социально-психологические последствия глобальных изменений природной среды. *Человек*, №3, 1995, с.97-104.

- средства, нелегально модифицирующие информационную среду, на основании которой человек принимает решения;
- средства создания виртуальной реальности;
- слухи;
- средства подпорогового психосемантического воздействия;
- средства генерирования акустических и электромагнитных полей.

Средства массовой информации и специальные средства информационно-пропагандистской направленности. СМИ наиболее эффективны для оказания информационно-психологического воздействия на большие массы людей, что позволяет рассматривать их как составную часть стратегических сил информационной войны. Использование различных технологий скрытого воздействия с помощью звука и видеоизображений на сознание и подсознание человека позволяет говорить о соответствии подобных средств по последствиям их применения с ОМУ.

Самой опасной чертой СМИ, считают многие специалисты, является их способность подавать информацию таким образом, чтобы за видимой объективностью у большой массы людей формировалась виртуальная картина реальности. Однако как только человек начинает сомневаться в виртуальной картине мира, эффективность информационно-психологического воздействия резко падает. Эти сомнения могут быть поддержаны технологиями контрпропаганды, также реализуемые с помощью СМИ.

Действенность СМИ как источника информационно-психологического воздействия обусловлена прежде всего созданием глобальных систем вещания. Имея вполне мирное и гуманное применение в повседневной жизни, они имеют возможность беспрепятственно довести сигнал до любой точки мира. Для многих регионов может оказаться, что данный источник информации является единственно доступным. Само обладание государством системами спутникового радио- и телевещания возможно будет служить сдерживающим или, наоборот, усиливающим фактором развязывания информационных войн.

Сила и результативность информационно-психологического воздействия, осуществляемых посредством СМИ и прежде всего телевидения, объясняются сильным психологическим эффектом сопричастия к событиям, когда человек погружается в них «здесь и сейчас». Этот своеобразный эффект, получивший название «эффект CNN», оценивается многими как главное условие эффективности информационно-психологического воздействия посредством СМИ.

К специализированным средствам информационно-пропагандистской направленности относятся мобильные радиовещательные и телевизионные центры, пропагандистские передвижные громкоговорители, плакаты, листовки. Технология их применения отработана и дальнейшее развитие связано прежде всего с методами скрытого воздействия на подсознание человека.

Глобальные компьютерные сети и программные средства быстрого распространения в сети пропагандистских информационных материалов. Развитие информационных и коммуникационных технологий привело к созданию уникального средства распространения информации — глобальной компьютерной сети интернет. Дешевизна доступа, свобода распространения и получения информации делает интернет эффективным инструментом для использования информационных механизмов воздействия на индивидуальное и массовое сознание.

В настоящее время группы различной политической ориентации и неправительственные организации могут использовать интернет для мобилизации политических сил против своего и других государств в кризисных ситуациях, чреватых неопределенным исходом. Неурегулированность правовых отношений при распространении информации в интернете влечет за собой свободу распространения клеветнической и недостоверной информации. Все это приводит к тому, что фактическая основа того или иного события может быть серьезно искажена посредством манипуляций с текстом, звуком и видеоизображением. Такие методы могут позволить широкому кругу заинтересованных лиц или групп реализовать сложный процесс управления общественным мнением или организовать крупные пропагандистские кампании для подрыва доверия граждан к конкретному курсу, проводимому правительством страны.

Вполне легальным способом информационно-психологического воздействия на пользователей интернета является распространение пропагандистских информационных материалов с помощью различных технологий привлечения внимания, организации виртуальных групп по интересам, сбора адресов электронной почты для организации массовых рассылок.

Создание различных виртуальных групп по интересам в интернете также служит легальным способом для проталкивания тех или иных идей. Образовавшаяся постоянная виртуальная группа свидетельствует о наличии людей, способных к восприятию продвигаемых идей, а рост

численности группы показывает эффективность информационно-психологического воздействия. Сложившаяся виртуальная общность людей может стать основой для образования реальных организаций террористического или криминального толка с трудно выявляемой структурой и системой связи.

Сбор адресов электронной почты в сети также создает основу для проведения целенаправленного воздействия на большие группы людей, поскольку позволяет создавать большие базы данных с информацией персонального характера, что дает возможность выделять группы влияния. В дальнейшем при необходимости этим группам можно высылать материалы пропагандистского характера.

Технологии быстрого распространения информации через компьютерные сети будут приобретать все большее значение, так как позволяют вполне легально проводить целенаправленные информационно-пропагандистские мероприятия без контроля со стороны государства, на население или отдельные группы граждан которого нацелено это информационно-психологическое воздействие.

Средства, нелегально модифицирующие информационную среду, на основании которой человек принимает решения. Деятельность человека все в большей степени опирается на возможности информационно-управляющих систем. Для решения практических задач человек старается сосредоточить в одном месте как можно больше информации для принятия более обоснованных решений. При всех преимуществах современных компьютеризированных систем поддержки принятия решений они обладают вполне очевидным недостатком — человек принимает решения на основе той информации, которую предоставляет ему система и достоверность которой в большинстве случаях он оперативно проверить не способен. Должностное лицо, принимающее решение, полностью полагается на ту информацию, которая выдается ему на монитор, поэтому внесение умышленных изменений в информационные массивы и сообщения влечет за собой неправильные решения. При большом количестве принимаемых решений и при большом потоке исходных данных доверие к информации означает доверие к правильности функционирования информационной системы в целом, т.е. протекающим в ней процессам сбора, обработки, хранения и отображения информации. Но доверие есть психологический фактор, поэтому некоторые приемы рефлексивного управления, направленные на формирование, укрепление или разрушение доверия могут быть интерпретированы как информационно-психологические воздействия.

В настоящее время во многих странах ведется разработка специализированных средств воздействия на информацию в информационно-управляющих системах. По достигаемому результату эти средства эквивалентны самым сильным технологиям информационно-психологического воздействия.

Средства создания виртуальной реальности. Мощь сетевых технологий умножается многократно благодаря новым технологиям мультимедиа и виртуальной реальности. Виртуальная реальность как имитация действительности может рассматриваться как психологический инструмент воздействия на сознание и подсознание человека. Она вовлекает его в новые формы существования и в определенной мере может формировать личность. Могут возникать и новые формы *опосредованного* социального контроля, основанные на замаскированном манипулировании сознанием, мягком подавлении психики, изменении структуры личности.

Социально-психологические последствия развития технологий виртуальной реальности, как и вообще современных символических визуальных систем, в контексте безопасности личности и общества могут быть негативны. Подобные технологии позволяют с максимальной эффективностью оказывать информационно-психологическое воздействие. Они часто используются для повышения наглядности подачи информации, например в программах новостей. Подобные технологии могут использоваться для создания любой реальной ситуации, сочетая элементы реального видеоизображения и элементы, созданные компьютерной графикой.

Есть сведения о разработке средств имитации голоса и видеоизображения политических и общественных лидеров. Появление лидера страны в неподобающем виде, произносящего непопулярные речи, может оказать, как считают специалисты, сильнейшее психологическое воздействие на население страны.

Обладание подобными техническими возможностями может рассматриваться как фактор в информационном противоборстве.

Слухи. Слухи являются неотъемлемым элементом в структуре неформальной коммуникации любого общества. Они представляют собой недостаточно проверенные сведения неизвестного происхождения, передаваемые в процессе межличностного общения.

Распространенность слухов в обществе свидетельствует о том, что они выполняют некоторые важные социальные функции. Они способствуют идентификации личности в социуме, с одной стороны, и повышают однородность мнений в группе, с другой. Внутригрупповое обсуждение слухов способствует кристаллизации общей точки зрения.

Слухи играют важную роль в конфликтах разного рода: межгрупповых, межнациональных, международных. Их значимость связана с тем, что в во многих случаях возможности воздействия конфликтующих сторон друг на друга существенно ограничены как законодательными рамками, так и общественным мнением. Кроме того, часто исход конфликта решается в процессе легитимизации наиболее распространенной в обществе точки зрения (выборы, референдумы). При этом возрастает значимость тех приемов информационно-психологического воздействия, которые связаны с изменением представлений о конфликте у большинства в направлении, выгодном для одной из конфликтующих сторон. Подобные изменения осуществляются при помощи специально подобранных сведений, распространяемых как по каналам СМИ, так и по каналам неформальной коммуникации. Именно по последним передаются слухи, которые становятся серьезным оружием в политическом или идеологическом столкновении. По сравнению с использованием СМИ использование неформальной коммуникации даже предпочтительнее, поскольку отсутствуют сведения об их авторе. Это уменьшает подозрения в политической ангажированности слуха и способствует тем самым его большей эффективности.

Средства подпорогового психосемантического воздействия. Современная наука предлагает широкий спектр способов управления поведением, мыслями и чувствами человека (или группы людей) через подпороговые психосемантические воздействия, например аудиовизуальное раздражение. Очень слабые, подпороговые, раздражители не воспринимаются сознанием. Однако, проникая в подсознание через слуховой и зрительный каналы, такие сигналы незаметно ориентируют мышление и поведение человека в заданном направлении. Например, на приятную для слуха мелодию посредством микшера накладывается повторяющийся словесный текст рабочего внушения, замедленный в 10-15 раз. Такой способ информационно-психологического воздействия может быть эффективно реализован по радио. Другой пример, при воздействии через зрительный канал (видеостимуляции) в запись видеофильма, например, вклинивают очень короткие (0,04 секунды) врезки картинок внушаемого текста или образа,

повторяемые каждые пять секунд. Техника изготовления кассеты несложная при минимальном наборе видеооборудования.

Методы и средства защиты от информационно-психологического воздействия

Цели и способы психологической защиты личности в традиционном смысле и защиты от информационно-психологического воздействия не вполне совпадают. Цель защиты — ослабление эмоционального напряжения, угрожающего индивиду. Защита личности от информационно-психологического воздействия в большей мере ориентирована на сохранение базовых свойств психики и нормальной духовности, индивидуальности характера, ценностных установок, нравственных критериев, свойств интеллекта и т.д.

Отсюда вытекает, что из известных в теории механизмов психологической защиты личности ведущим для информационно-психологического воздействия является интеллектуализация. Лишь глубокий анализ информационной ситуации (естественно, при условии достаточно высоких уровней других характерологических компонентов личности) позволяет выявить манипулятивный характер информационно-психологического воздействия, оценить достоверность информации и выработать наиболее приемлемые для конкретного индивида способы защиты от нежелательных последствий. Стоит заметить, что имманентно присущие человеку защитные свойства личности формируются в процессе жизненного опыта, воспитания и самовоспитания.

Сложнее обстоит дело со способами психологической защиты от информационно-психологического воздействия больших масс людей. Естественно, что чем больше в этой массе будет индивидов с хорошей личностной защитой, тем устойчивее окажется и сама масса (социум). Но здесь есть значительная специфика. Она заключается в том, что у социума, во-первых, должен быть высокий позитивный самообраз «Мы», а во-вторых, должна быть невысокая внушаемость и «заражаемость», свойственная толпе[8]. Позитивный самообраз «Мы» формируется, в первую очередь, на основе самоидентификации людей с определенным социальным окружением. Самоидентификация есть всегда фактор политический. Для современной России самоидентификация означала бы наличие у населения сильно выраженного сознания того, что «Я — гражданин России, Я горжусь этим и Я солидарен с другими гражданами».

[8] Московичи Серж. Век толп. Исторический трактат по психологии масс. Пер. с фр. Центр психологии и психотерапии. М., 1996.

Следует, однако, иметь в виду, что не все информационно-психологические воздействия являются опасными. Более того, некоторые из них могут быть полезными для повышения устойчивости населения к деструктивным информационно-психологическим воздействиям, для повышения популяционного психологического потенциала. Это информационно-психологическое воздействие, направленное на укрепление социального характера, на психологическую мобилизацию населения для преодоления общих для социума трудностей, например в условиях войны, природных или социальных бедствий и т.п.

ГЛАВА 3. ИНФОРМАЦИОННОЕ ОРУЖИЕ КАК НОВОЕ СРЕДСТВО ВООРУЖЕННОЙ БОРЬБЫ

Информационное оружие — продукт новых информационных технологий

В результате широкого применения новых информационных технологий претерпели изменения не только средства вооруженной борьбы, но и стратегия, и тактика ведения современных войн, появились новые концепции ведения боевых действий в «информационный век», учитывающие новые факторы уязвимости сторон. Эти новые концепции непосредственно увязываются с тем, что стремительная эволюция киберпространства может не только открыть дополнительные возможности качественного совершенствования вооружения и военной техники, но и обусловить возникновение новых проблем уязвимости противоборствующих сторон: в современных условиях более уязвима та из воюющих сторон, которая имеет меньше информации о поле боя, медленнее обрабатывает информацию и принимает решения с меньшей оперативностью. Если ранее в войнах существенные недостатки тактической информации можно было компенсировать привлечением дополнительных сил, то в настоящее время информационное превосходство практически однозначно предопределяет исход современного скоротечного вооруженного конфликта.

Неуклонно возрастает зависимость процессов, происходящих в различных областях военной деятельности, от качества функционирования информационно-телекоммуникационных систем. Эффективность функционирования большинства современных средств вооруженной борьбы определяется, в первую очередь, возможностями обеспечивающих их деятельность автоматизированных систем управления и связи. Появляется широкий спектр методов и средств воздействия на подобные системы путем вывода из строя их отдельных структурных элементов, ключевых операторов или манипуляции информацией в них в интересах заинтересованных сторон. При этом сам конфликт в стадию открытого вооруженного столкновения может и не перейти, а завершиться уже после этапа «информационного противоборства», результатом которого станет осознание одной из противоборствующих сторон, что она не может больше рассчитывать на эффективное применение своих средств вооруженной борьбы. В любом случае сторона, лучше владеющая стратегией и тактикой ведения военных действий в информационном пространстве (информационной

войны), будет в современных условиях иметь существенные преимущества.

При рассмотрении понятия «информационная война», как правило, выделяется две ее составляющие: наступательная и оборонительная. Наступательная информационная война предполагает использование разнообразных средств и методов воздействия на информационные системы противника в целях снижения эффективности функционирования его системы принятия решений. При этом средства и методы, наиболее эффективные для такого воздействия получили название «информационное оружие». Целью проведения подобных наступательных операций, как и прежде, остается стремление к ослаблению и достижению победы над вероятным противником. Однако наличие новых средств и методов воздействия на ключевые элементы гражданской и военной инфраструктуры противника, а также на его личный состав существенно изменяет их принципы, тактику и допустимые условия проведения.

Оборонительные информационные операции включают в себя проведение различных мероприятий с использованием средств и методов противодействия эффективному применению информационного оружия противником. Особенностью информационной войны является необходимость одновременного проведения как наступательных, так и оборонительных мероприятий.

В качестве информационного оружия может выступать совершенно различное вооружение: высокоточное оружие для поражения органов управления или отдельных радиоэлектронных средств, средства радиоэлектронной борьбы (РЭБ), источники мощного электромагнитного импульса, программные вирусы и др. Критерием отнесения к разряду «информационного оружия» может рассматриваться только эффективность того или иного вооружения при решении задач информационной войны.

Наступательная операция с использованием информационного оружия (информационная наступательная операция) может проводиться как самостоятельно, так и в комплексе с традиционными наступательными действиями, либо предшествуя им, либо поддерживая их проведение. В любом случае информационная наступательная операция призвана обеспечить «информационное превосходство» в ходе конфликта за счет воздействия на средства сбора информации, ее переработки и хранения, а также на личный состав, обслуживающий технику и принимающий решения.

Информационное превосходство не является самоцелью, так как оно предоставляет преимущество только в случае его эффективного преобразования в превосходство в области осведомленности и принятия решений. Именно в этом случае появляется возможность вырабатывать лучшие решения и воплощать их в жизнь быстрее, чем противник может на них отреагировать. В американском документе «Joint Vision 2020», в котором изложены взгляды Комитета начальников штабов США на формы и способы ведения войны в период до 2020 г., подчеркивается, что информационное превосходство по своей природе не постоянно и оно должно создаваться и поддерживаться объединенными силами путем проведения информационных наступательных операций.

Развитие информационных технологий существенно меняет технические возможности систем управления войсками (силами), что повлечет за собой активизацию исследований в области практической реализации концепции «информационная война» и расширит спектр НИОКР в области информационного оружия. По оценкам американских специалистов, существенной угрозой является расширение возможности доступа ряда стран к средствам космической разведки (цифровым картам), обеспечивающим разрешающую способность пять метров и менее. При таком уровне разрешения появляется возможность распознавать ключевые элементы инфраструктуры противника и наводить на них крылатые или баллистические ракеты, особенно если при этом используется глобальная навигационная система.

Высокоскоростная передача больших массивов информации становится самой важной задачей при создании современных систем управления, решение которой связывается с развитием космических систем связи и широким использованием волоконно-оптических линий. При этом подобные элементы информационной инфраструктуры становятся наиболее уязвимыми с точки зрения информационной наступательной операции.

Концентрация ресурсов в рамках ограниченного числа элементов глобальной (локальной) информационной инфраструктуры ведет, с одной стороны, к уязвимости всей системы в целом при наличии соответствующих средств поражения. С другой стороны, возможности информационной инфраструктуры таковы, что даже вывод из строя относительно большого количества ее элементов, может снизить эффективность выполнения критически важных информационных процессов, т.е. значительный вывод из строя информационной

инфраструктуры либо воспрепятствование доступу к ней возможны только на непродолжительный промежуток времени. Целенаправленная организация подобных ситуаций и является приоритетной задачей при применении информационного оружия в ходе ведения наступательной информационной войны и достижения информационного превосходства над противником. Эффективное противодействие такого рода действиям противника определяет цель оборонительной информационной войны.

Классификация информационного оружия

В настоящее время не существует устоявшейся классификации информационного оружия, так же как и четкого определения самого этого понятия[1]. Исходя из общих соображений к информационному относят оружие, наиболее эффективно решающее задачи информационной войны. При этом следует добавить, что информационное оружие должно способствовать достижению военного превосходства нетрадиционным образом, исключая массированное физическое поражение и ориентируясь на высокоточные и максимально скрытные нелетальные способы воздействия.

Виды и типы информационного оружия

По своему целевому назначению информационное оружие делится на оборонительное и наступательное. Оборонительное информационное оружие решает задачи оборонительной информационной войны и представляет собой системы многоуровневой компьютерной безопасности и различные системы активного противодействия информационному оружию противника. Наступательное информационное оружие предназначено для воздействия на противника путем поражения его наиболее критичных структур системы обеспечения цикла принятия решений[2].

С теоретической точки зрения можно выделить следующие виды информационного оружия (табл. 1):

- средства высокоточного местоопределения оборудования, излучающего в электромагнитном спектре, и его огневого поражения

[1] В Приложении 1 дано три наиболее, с нашей точки зрения, подходящих определения. Общее их количество в литературе оценить трудно.

[2] Организационно-техническая система, реализующая цикл принятия решений, включает в себя пункты и органы управления, систему автоматизации управления, систему связи, специальные системы сбора и обработки развединформации, датчики. Снижение эффективности подобной территориально распределенной системы возможно либо за счет изменения ее структуры, либо воздействия на ее ресурсы: вычислительные, программные, информационные, связные или личный состав.

путем оперативного выявления отдельных элементов информационной системы управления, распознавания, наведения и огневого поражения;
- средства воздействия на компоненты радиоэлектронного оборудования и их энергопитание для временного или необратимого вывода из строя отдельных компонентов радиоэлектронных систем;
- средства воздействия на программный ресурс электронных управляющих модулей, обеспечивающие вывод их из строя либо изменение алгоритма их функционирования посредством использования специальных программных средств;
- средства воздействия на процесс передачи информации, которые предназначены для прекращения или дезорганизации функционирования подсистем обмена информацией за счет воздействия на среду распространения сигналов и алгоритмы функционирования;
- средства пропаганды и дезинформации для внесения изменений в информацию систем управления, создание виртуальной картины обстановки, отличной от действительности, изменение системы ценностей человека, нанесение ущерба духовно-нравственной жизни населения противника;
- психотронное оружие, предназначенное для воздействия на психику и подсознание человека с целью снижения и подавления его воли, временного вывода из строя, зомбирования.

Нельзя утверждать, что данная классификация охватывает все виды информационного оружия, появление которых возможно в будущем. Однако все известные практические разработки, проводимые в настоящее время, полностью ею охватываются.

Информационное оружие каждого вида можно классифицировать по ряду признаков:
- одно- и многоцелевое или универсальное;
- ближнего и дальнего радиуса действия;
- индивидуального, группового или массового поражения;
- по типу носителя;
- по эффекту поражения.

По типу воздействия информационное оружие можно разделить на три категории: оружие, основанное на информационных технологиях, оружие, оказывающее энергетическое и химическое воздействие.

Примерами информационного оружия, основанного на *энергетическом воздействии*, являются:

- высокоточные самонаводящиеся боеприпасы, включая специализированные крылатые ракеты и ударные беспилотные летательные аппараты;
- средства силового радиоэлектронного подавления, сверхмощные генераторы СВЧ, средства силового воздействия через электросеть;
- средства РЭБ наземного и воздушного базирования, забрасываемые передатчики помех одноразового использования;
- специальные генераторы излучения, воздействующие на психику человека.

В качестве примеров информационного оружия, в основе которого лежит *химическое воздействие*, можно привести следующие средства: боеприпасы, оснащенные газами, аэрозолями или биологическими культурами, разрушающими компоненты радиоэлектронной аппаратуры, специальные фармакологические средства и специально структурированные лекарства психотронного ряда, оказывающие негативное влияние на психику человека.

Наиболее перспективным считается использование в качестве информационного оружия *информационных технологий*. Информационные технологии являются неотъемлемой частью высокоточных боеприпасов, так как их наведение обеспечивается системами местоопределения и доразведки по визуальным, радиолокационным и другим демаскирующим признакам. Поэтому и эти функциональные подсистемы целесообразно рассматривать также в качестве информационного оружия.

Наиболее традиционным и мощнейшим универсальным информационным оружием является *пропаганда*, осуществляемая с использованием СМИ.

В настоящее время активно разрабатывается информационное оружие на основе *программного кода*.

К информационному оружию также относятся средства, реализующие технологии зомбирования и психолингвистического программирования.

В табл. 1 представлена предлагаемая классификация информационного оружия по видам и типам. Выделение типов информационного оружия в некоторой степени условно, потому что подобное оружие в реальной обстановке будет применяться комплексно и создаваться в виде полуавтоматизированного набора различных специализированных средств, требующего для эксплуатации разумного уровня квалификации персонала.

Таблица 1. Классификация информационного оружия

Виды информационного оружия	Назначение	Возможные типы информационного оружия	
		На основе энергетического и химического воздействия	На основе информационных технологий
Средства высокоточного местоопределения оборудования, излучающего в электромагнитном спектре, и его огневого поражения	Оперативное выявление отдельных элементов информационной системы управления, распознавание, наведение и огневое поражение с целью физического уничтожения	Высокоточные боеприпасы с самонаведением на средства связи с использованием всех видов демаскирующих признаков. Высокоточные средства поражения на основе целеуказания и ориентации с помощью высокоточной навигационной системы	Средства высокоточного местоопределения (в том числе и когерентных источников). Средства доразведки по визуальным, радиолокационным и другим демаскирующим признакам
Средства воздействия на компоненты радиоэлектронного оборудования и их электропитание	Временный или необратимый вывод из строя отдельных компонентов радиоэлектронных систем	Средства силового радиоэлектронного подавления: сверхмощные генераторы СВЧ (гиротроны, рефлектные триоды, релятивистские магнитроны, тубутроны); взрывомагнитные генераторы; взрывные магнитогидродинамические генераторы. Средства силового воздействия через электросеть. Средства вывода из строя электросетей	Программные средства вывода из строя оборудования (резонанс головок жестких дисков, выжигание мониторов и др.). Программные средства стирания перезаписываемой памяти. Программные средства воздействия на бесперебойные источники питания и др.
Средства воздействия на программный ресурс электронных управляющих модулей	Вывод из строя либо изменение алгоритма функционирования программного обеспечения уп-		Средства преодоления систем защиты информации. Средства проникновения в информационные сети противника. Средства маскировки источников получения информации.

	равляющих систем посредством использования специальных программных средств		Средства вывода из строя всего либо конкретного программного обеспечения информационной системы, возможно в строго заданный момент времени или при наступлении определенного события в системе. Средства скрытого частичного изменения алгоритма функционирования программного обеспечения. Средства сбора данных, циркулирующих в информационной системе противника. Средства доставки и внедрения определенных алгоритмов в конкретное место информационной системы. Средства воздействия на системы охраны объектов.
Средства воздействия на программный ресурс электронных управляющих модулей	Прекращение или дезорганизация функционирования подсистем обмена информацией за счет воздействия на среду распространения сигналов и алгоритмы функционирования	Средства РЭБ, особенно наземные, воздушные (вертолетные и беспилотные летательные аппараты) станции помех радиосвязи (возможно с элементами искусственного интеллекта). Забрасываемые передатчики помех одноразового использования	Средства воздействия на протоколы передачи данных систем связи и передачи данных. Средства воздействия на алгоритмы адресации и маршрутизации. Средства перехвата и нарушения прохождения информации в технических каналах ее передачи. Средства вызова перегрузки системы ложными запросами на установление связи.
Средства психологического воздействия, пропаганды и дезинформации	Внесение изменений в информацию систем управления, создание виртуальной картины обста-		Информационные технологии СМИ, пропаганда, клевета. Средства создания или модификации виртуальной реальности. Средства имитации голосов операторов систем управления (например,

	новки отличной от действительности, изменение системы ценностей человека, нанесение ущерба духовно-нравственной жизни населения противника		систем управления воздушным движением) и видеоизображения конкретных людей с их голосом (лидеров партий и стран). Средства модификации информации, хранимой в базах данных информационных систем противника. Средства ввода в информационные системы противника ложной информации и данных (например, целеуказания или мест доставки грузов). Средства дезинформации охранных систем. Средства модификации данных навигационных систем, систем метеообеспечения, систем точного времени и др.
Психотронное оружие	Воздействие на психику и подсознание человека с целью снижения его воли, подавление, временный вывод из строя, зомбирование	Психофармакологические. Психодислептические. Транквилизаторы. Антидепрессанты. Галлюциногены. Наркотики. Специально структурированные лекарства. Специальные генераторы излучения, воздействующего на психику человека	Специальная видеографическая и телевизионная информация (25 кадр, повышение давления, вызов эпилептических припадков и др.). Средства создания виртуальной реальности, подавляющей волю и вызывающей страх (проецирование на облака изображения «бога» и др.). Технологии зомбирования и психолингвистического программирования

Характеристики информационного оружия

Информационное оружие на основе энергетического воздействия. Для поражения средств связи обычными боеприпасами и высокоточным оружием большое значение имеет точность целеуказания средствами радио- и радиотехнической разведки. В настоящее время наземные и воздушные комплексы радио- и радиотехнической разведки, находящиеся на вооружении и работающие в диапазоне от 0,5 ГГц и выше, имеют точность определения координат, достигающую 0,06-0,1% от дальности. Дальность разведки примерно равна дальности прямой видимости для авиационных средств и 30-35 км для наземных. Такая точность является достаточной для целеуказания средствам огневого поражения (ствольной и реактивной артиллерии, авиации).

Для увеличения дальности и точности целеуказания создаются многопозиционные наземно-авиационные системы местоопределения, использующие разностно-временные, доплеровские, фазовые и комбинированные методы местоопределения. Одной из целей работ является повышение точности определения координат радиоэлектронной системы до величины, достаточной для вывода в район цели средств высокоточного оружия и их носителей. В дальнейшем цели могут быть доразведаны по визуальным, радиолокационным и другим демаскирующим признакам. Высокоточное оружие при поражении связных радиоэлектронных систем может наводиться на их собственное функциональное радиоизлучение, на паразитные (более высокочастотные) излучения, а также на сопутствующие радиоэлектронные системы тепловые излучения, например ИК-излучения дизельгенераторов.

Разрабатываемые в настоящее время высокоточные боеприпасы нового поколения будут обладать способностью наводиться на средства связи с использованием всех видов их демаскирующих признаков. В частности, в США создается специальная крылатая ракета с большой длительностью полета, предназначенная для уничтожения важных радиоэлектронных систем, включая радиоэлектронные системы связи, путем самонаведения на их излучение. Предполагается, что такие ракеты будут по данным радио- и радиотехнической разведки запускаться в район цели и, барражируя в нем, самостоятельно производить поиск, распознавание радиоэлектронных систем и самонаводиться на его уязвимые элементы. Аналогично предполагается использовать и малогабаритные ударные беспилотные летательные аппараты, наведение при этом будет осуществляться по данным бортовых средств радио- и радиотехнической разведки, тепло- и телевизионной аппаратуры.

Одновременно Министерство армии США разрабатывает семейство унифицированных наземных и авиационных (на вертолетах и беспилотные летательные аппараты) станций помех радиосвязи с элементами искусственного интеллекта, которое должно в период до 2005 г. заменить на вооружении существующие средства.

Создается малозаметный ударный беспилотный летательный аппарат для нанесения ударов по наземным целям (командные пункты, радиолокационные станции (РЛС), пусковые установки зенитных управляемых ракет) одной или двумя небольшими авиабомбами с последующим возвращением в место базирования. Для ударных беспилотных летательных аппаратов разрабатывается новое информационное оружие (неядерные генераторы электромагнитных импульсов, бомбы, снаряженные токопроводящими волокнами и т.п.) для вывода из строя компьютеров и систем электроснабжения.

Применение современных средств РЭБ сталкивается с определенными трудностями идентификации источников излучения радиолокационного диапазона. Это связано со значительными различиями в конструкции и способах применения РЛС и тем, что современные РЛС получили возможность изменять характеристики излучаемых сигналов непосредственно в процессе работы.

Особое беспокойство специалистов в области средств радиотехнической разведки вызывает появление РЛС непрерывного частотно-модулированного излучения с низкими демаскирующими признаками, таких как голландская «Скаут» и шведская «Пилот МК-2».

Большое значение придается совершенствованию забрасываемых передатчиков помех одноразового использования.

В предстоящие годы, вероятно, будут значительно усовершенствованы передатчики одноразового использования для подавления радиоэлектронных систем, в частности за счет оснащения их собственными средствами разведки и элементами искусственного интеллекта для самостоятельного обнаружения и идентификации целей, выбора объекта и оптимальных режимов подавления, наведение передатчика помех, выполнение функций контроля эффективности подавления, слежение за целью по частоте и параметрам модуляции сигналов.

Эффективность воздействия передатчиков одноразового использования возрастет также за счет повышения точности их доставки к цели (это в свою очередь облегчает их поиск и уничтожение, для противодействия которым предполагается применять кратковременные и скрытые режимы работы - ретрансляционные помехи, помехи, маскируемые под действие естественных радиофизических факторов, под взаимные помехи своих радиоэлектронных систем и т.п.) и увеличения времени работы.

Наряду с совершенствованием средств активных помех связи традиционных типов активно ведутся работы по созданию качественно новых средств силового радиоэлектронного подавления, вызывающих подавление или полный вывод из строя радиоэлектронных схем или реализующих помеховое воздействие на радиоэлектронные системы за счет паразитных каналов приема, нелинейных эффектов и т.п. Такие средства характеризуются мощностью помехового сигнала на входе подавляемого на радиоэлектронные системы, на несколько порядков превышающей уровень полезного, и занимают промежуточное положение между традиционными средствами РЭБ и СВЧ-оружием.

Средства силового радиоэлектронного подавления могут быть реализованы также в виде маломощной разновидности пучкового (ускорительного) оружия. Основные трудности на пути создания таких средств связаны с тем, что:

- в мире недостаточно изучены механизмы поражения СВЧ-излучением радиоэлектронных компонентов;
- существующие и разрабатываемые сверхмощные генераторы СВЧ не полностью отвечают предъявляемым требованиям;
- мощные источники питания малопригодны для использования в полевых условиях.

В настоящее время основными направлениями работ в области сверхмощных генераторов СВЧ являются:

- увеличение выходной мощности генераторов традиционного типа (клистроны, магнетроны и т.п.);
- разработка генераторов принципиально новых типов на основе релятивистских электронных пучков (гиротроны, лазеры на свободных электронах и др.), генераторов с виртуальным катодом (виркаторов, турбутронов, рефлексных триодов и др.);
- создание одноразовых и многоразовых генераторов, использующих преобразование химической энергии взрывчатого вещества в энергию электромагнитного поля (взрывомагнитные генераторы, взрывные

магнитогидродинамические генераторы и т.п.) и совершенствование пучково-плазменных генераторов.

Весьма перспективными для использования в средствах силового радиоэлектронного подавления являются взрывомагнитные генераторы. Их принципиальным достоинством является возможность доставки непосредственно в район подавляемой цели.

Одним из отрабатываемых способов генерации мощных СВЧ-импульсов является использование ускорителей электронов, обеспечивающих получение мощного направленного СВЧ-излучения при взаимодействии пучка релятивистских электронов с плазмой. В экспериментах были получены поля с напряженностью 104 В/м.

Еще одним перспективным направлением создания СВЧ генераторов и источников питания для средств силового радиоэлектронного подавления является использование взрывных магнитогидродинамических генераторов, непосредственно преобразующих энергию взрывчатого вещества в электрическую. По некоторым прогнозам, они могут обеспечить мощность несколько тысяч гиговатт, энергию импульса порядка мегаджоуля при частоте их повторения до 100 Гц.

На стадии исследований и испытаний находятся электромагнитные генераторы с выходной мощностью более 100 МВт, энергией импульса 10-1000 Дж, длительностью импульса 10-100 нс и периодичностью импульсов 100-1000 Гц. В ближайшей перспективе ожидается создание электромагнитной бомбы с эффективным радиусом поражения 1000 м и более.

Сверхмощные генераторы СВЧ планируется использовать на базе беспилотных летательных аппаратов для вывода из строя системы ПВО противника или органов управления. Предполагается, что ресурса вылета одного беспилотного летательного аппарата с генератором хватит на 100 тыс. импульсов. На одну цель планируется затрачивать до 1000 импульсов для повышения вероятности ее поражения. За одни вылет беспилотный летательный аппарат сможет поразить до 100 целей.

Исследуется использование сверхмощных генераторов СВЧ для поражения противника в ближнем бою и разминирования. Высказывается мнение, что это оружие может быть использовано и против ядерного оружия для его дезактивации. Практические образцы СВЧ генераторов

обеспечивают при весе 20 кг импульс мощностью 1 ГВт. При весе 200 кг генератор обеспечивает мощность 20 ГВт. Наиболее удобным носителем для доставки до цели таких средств считается беспилотный летательный аппарат.

Большие возможности для воздействия на военные системы и средства управления открывает все расширяющееся использование в них вычислительной техники, особенно пространственно распределенных сетей ЭВМ. ЭВМ как электронные устройства подвержены всем основным способам воздействия, рассмотренным в настоящем разделе, хотя их защищенность, ввиду отсутствия функциональных узлов для приема электромагнитного излучения, как правило, выше, чем у других типов радиоэлектронной аппаратуры.

Информационное оружие на основе химического воздействия. Использование различных газов, аэрозолей и биологических культур для поражения радиоэлектронных компонентов неоднократно обсуждалось на страницах иностранной прессы. Указывались теоретические возможности различных средств в данной области. Однако достоверных сведений о практических результатах в этой области в настоящее время неизвестно.

Информационное оружие на основе программного кода. Возможность создания и практического применения информационного оружия на основе программного кода в настоящее время не оспаривается. Известны и случаи его практического применения. По оценкам американских специалистов, их информационные ресурсы подвергаются ежегодно более чем четверти миллиона атак со стороны анонимных пользователей. При этом считается, что регистрируется примерно один процент всех реально проведенных атак. Однако следует заметить, что при этом не дается пояснений, какого уровня воздействия считаются атаками.

Доставка до цели информационного оружия на основе программного кода может осуществляться различными способами:

- самораспространением вирусоподобных оболочек; наиболее совершенные вирусы используют алгоритмы вскрытия системы защиты и распространяются в информационных сетях самостоятельно (так называемые «черви»);
- переносом другим часто используемым программным обеспечением, при инициализации которого начинает функционировать информационное оружие (собственно программные вирусы);

- различными средствами долговременного хранения информации, в том числе перепрограммируемыми микросхемами (прошивка постоянного запоминающего устройства).
- заранее внедренными закладками, получившими название «троянский конь»;
- дистанционным внедрением программного кода через порты приема информации.

Подобное информационное оружие позволяет осуществлять:
- вывод из строя оборудования электронных систем за счет ввода головок жестких дисков в резонанс или выжигания устройств наглядного отображения;
- стирание перезаписываемой памяти;
- перевод в угрожающие режимы работы бесперебойных источников питания или отключение их защитных функций;
- маскировка источников получения информации;
- вывод из строя всего либо конкретного программного обеспечения информационной системы, возможно в строго заданный момент времени или при наступлении определенного события в системе;
- скрытое частичное изменение алгоритма функционирования программного обеспечения;
- сбор данных, циркулирующих в информационной системе противника;
- доставку и внедрение определенных алгоритмов в конкретное место информационной системы;
- воздействие на протоколы передачи данных систем связи и передачи данных;
- воздействие на алгоритмы адресации и маршрутизации в системах связи и передачи данных;
- перехват и нарушение прохождения информации в технических каналах ее передачи;
- блокирование системы;
- имитацию голосов операторов систем управления (например, систем управления воздушным движением) и создание виртуальных видеоизображений конкретных людей с их голосом (лидеров партий и стран);
- модификацию информации, хранимой в базах данных информационных систем противника;
- ввод в информационные системы противника ложной информации и данных (например, целеуказания или мест доставки грузов);
- дезинформацию охранных систем;

- модификацию данных навигационных систем, систем метеообеспечения, систем точного времени и др.;
- негативное воздействие на человека посредством специальной видеографической и телевизионной информации;
- создание или модификация виртуальной реальности, подавляющей волю и вызывающей страх (проецирование на облака изображения «бога» и др.).

Признавая важность и сложность проблемы защиты от информационного оружия, в бюджете Министерства обороны США на 2000 финансовый год было дополнительно выделено 515 млн долл. для защиты вычислительных сетей информационной инфраструктуры. При разработке технологий защиты информации активно используется интернет, позволяющий за счет использования специальных средств (например, системы «Хищник») с пункта прослушивания в любой точке земного шара проникать в персональные компьютеры без физического доступа к ним и добывать информацию, размещая скрытое программное обеспечение. Однако на практике этот метод используется, главным образом, для контроля домашних компьютеров чиновников.

Другая технология предусматривает маркировку электронных документов, хранимых на жестком диске компьютера. При попытке открыть промаркированный документ, автоматически об этом посылается сообщение в центр управления, который может находиться в любой точке земного шара. Данный документ может сопровождаться через множество защитных экранов по всему миру для фиксации местоположения получателя.

Агентство национальной безопасности США получило патент на систему распознавания речи, которая должна стать инструментом контроля голосового трафика и данных за счет маркировки речи в сетях интернет и при обнаружении атаки проводится процедура анализа данных, достаточных для открытия уголовного дела, сбора доказательств и выявления автора атаки. Кроме того, для Министерства обороны и частного сектора разрабатывается автоматическая среда обнаружения проникновений.

Информационное оружие на основе средств воздействия на психику. В общем контексте информационной войны и создания информационного оружия приобретает особую актуальность проблема изучения психологического воздействия[3]. По мнению психологов, несмотря на

[3] Подробно рассмотрено в пункте «Информационно-психологическая безопасность», глава 2.

широкое внедрение компьютерной техники и доведение процесса автоматизации до высокого интеллектуального уровня, человек по-прежнему остается высшим управляющим звеном, отвечающим за принятие окончательных решений. Специалисты считают, что в условиях, когда человек вынужден ориентироваться в условиях недостатка информации, либо ее избытка, повышается вероятность принятия ошибочных решений с последующим накоплением ошибок на различных уровнях управляемого процесса.

Более того, объем, интенсивность, способы и формы подачи информации, их несогласованность с возможностями сенсорных систем восприятия в соответствующих структурах головного мозга могут привести к значительным перегрузкам, выражающимся в потере способности правильно оценивать ситуацию и торможении всей нервной системы. Это является одной из причин того, что человек, принимающий решения, в нынешних условиях становится приоритетным объектом информационно-психологического воздействия в информационной войне.

Ряд исследователей склонны рассматривать информационно-психологические методы в качестве альтернативных стратегических средств воздействия на противника. Подобные мероприятия могут проводиться как с целью его сдерживания (либо обеспечения собственной безопасности), так и с целью вызова процесса саморазрушения противостоящей социальной системы. И в данном контексте иррациональные мотивы, возникающие в подсознании лиц, принимающих решения, отодвинув на задний план рациональные расчеты и соображения, могут сыграть ключевую роль. Таким образом, наряду с экономическим воздействием на противника, психологическая война, построенная на использовании иррациональных мотивов возбуждения внутрисистемной конфликтности, является эффективным средством достижения политических и военных целей.

Информационное оружие на основе информационных технологий. Возможность создания психотронных средств на основе информационных технологий активно обсуждается в печати, однако о реальных НИОКР в этой области не известно. Активизация обсуждения данного вопроса последовала после сообщений японских СМИ о том, что 12 декабря 1997 г. по национальному телевидению Японии демонстрировался мультфильм, содержащий контаминацию цветовой гаммы, звука, мигания визуальной информации, от просмотра которого

десятки людей получили психофизические расстройства различной тяжести. Работы по использованию «25 кадра» проводятся давно. Однако дальше экспериментов они, видимо, не продвинулись.

Средства информационного воздействия на живую силу классифицируются на средства информационно-психологического и энергоинформационного воздействия. Отличие этих видов оружия заключается в следующем.

Информационно-психологическое оружие воздействует через сознание на психику человека в основном с помощью СМИ, компьютерных игр и т.п. Перспективы совершенствования подобных средств определяются общими тенденциями в развитии технологий и средств массовой информации, гипноза, нейролингвистического программирования и др.

Энергоинформационное оружие воздействует через физиологию на психическое состояние человека, минуя его сознание. Человек не осознает факта воздействия, но в зависимости от режима облучения начинает ощущать или бодрое, радостное состояние, уверенность в себе и в будущем, или подавленное, мрачное, тревожное состояние, страх, неуверенность и обусловленную этим агрессивность.

Функционирование энергоинформационного оружия базируется на методах лечебной физиотерапевтической практики. Обобщение и анализ результатов лечения физиотерапевтическими методами показывает, что облучение пациентов с неврозом возбуждения излучением с длиной волны 2 мм и частотой модуляции 2 Гц при продолжительности сеанса 10 мин приводило к существенному улучшению состояния пациентов. При лечении пациентов с неврозом торможения положительные результаты достигались при тех же параметрах излучения, но при частоте модуляции 20-21 Гц. При проведении лечения наблюдалась стабилизация состояния пациентов примерно к четвертому-пятому сеансу.

Облучение здоровых людей подобными излучениями с отмеченными параметрами обусловливает опасность их перевозбуждения при частоте модуляции 20-21 Гц и подавленности — при частоте 2 Гц. Вследствие этого появляется возможность дистанционного управления психофизическим состоянием и поведением облучаемых людей путем низкоэнергетического (не более 50 мкВт/см^2) энергоинформационного воздействия. Такие процессы могут быть специально организованы путем низкочастотной модуляции генерируемых СВЧ.

Отмеченные особенности энергоинформационного воздействия могут быть использованы в целях изменения поведения людей и управления социальными установками региональных и глобальных социумов. В частности, с помощью энергоинформационного воздействия теоретически можно «разжечь» или «притушить» накал забастовочного движения, демонстраций, беспорядков и тем самым оказать влияние на социальные, политические (например, выборы властных структур), экономические (срыв производства и т.п.) процессы и военные действия.

Гипотетически механизм такого воздействия реализуется следующим образом. Подавая положительные сведения о своем претенденте на какую-либо должность через СМИ и одновременно создавая с помощью энергоинформационного воздействия хорошее психофизическое состояние населения, можно выработать у населения положительный условный рефлекс на этого претендента и за счет этого существенно повысить его популярность.

Подавая негативную информацию о нежелательном претенденте и одновременно создавая отрицательное психофизическое состояние людей с помощью энергоинформационного воздействия, можно выработать отрицательный условный рефлекс на этого претендента. Ухудшая психофизическое состояние личного состава войск, можно существенно снижать их боеспособность вплоть до сдачи в плен. И наоборот, улучшая психофизическое состояние своих войск, можно существенно повысить их боеспособность.

Информационное воздействие на человека сравнительно малых мощностей СВЧ-излучения практически не изучено. В 70-х годах сообщалось об открытии в США так называемого эффекта радиослышимости. Эффект якобы заключался в том, что люди, находившиеся в мощном поле вещательных станций, начинали слышать «внутренние голоса», музыку и тому подобное. Наличие эффекта объяснялось возможностью детектирования радиосигналов во внутренних средах организма человека с последующим преобразованием в сигналы, воспринимаемые слуховым нервом. В ходе проведенных в первой половине 70-х годов исследований были якобы выявлены пороговые мощности возникновения эффекта в СВЧ диапазоне в импульсном режиме. Однако в дальнейшем сообщения о радиослышимости не подтверждались, хотя и не опровергались. Вновь об этом заговорили только в 1997 г. в связи с успешными испытаниями РЛС для разгона скоплений птиц вблизи взлетно-посадочных полос

аэродромов. В ходе экспериментов установлено, что при правильной модуляции радиоимпульсы с крутыми фронтами вызывают появление на барабанной перепонке уха небольших тепловых импульсов, воспринимаемых мозгом человека как звуковые сигналы. Этот эффект, в случае его реального существования, вероятно, можно было бы использовать в качестве информационного оружия для психологической обработки личного состава и населения. Путем передачи слуховых эффектов непосредственно в мозг при облучении людей модулированным СВЧ-излучением появляется возможность зомбирования населения. Учитывая, что эти слуховые эффекты воспринимаются изнутри, т.е. как внутренние убеждения, доверие к ним у людей больше, чем к поступающей внешней информации. Следовательно, и эффективность такого воздействия будет больше.

Таким образом, появляется возможность дистанционного управления людьми, влияния на их действия во время выборных компаний, боевых действий, чрезвычайных ситуаций, террористических актов, массовых волнений и других подобных действий. При этом перед обладателем средств энергоинформационного воздействия открывается возможность реализации гегемонии управления всеми происходящими социально-политическими и экономическими процессами и установления своего режима. Для реализации всех отмеченных процессов, как показано выше, необходимо лишь изменять частоту модуляции излучений, что технически вполне реализуемо.

Исследования показали, что целенаправленное воздействие может осуществляться через СМИ путем создания специальных звуковых сигналов, музыкальных шлягеров, ключевых видеообразов телепрограмм, голографических изображений в пространстве, а также путем облучения модулированным электромагнитным излучением (психотронное воздействие).

Следует также отметить наличие информации о возможности создания компьютерных вирусов-убийц. Так, был зарегистрирован и идентифицирован случай смерти человека от кровоизлияния в мозг, вызванного вирусом с названием «666». Воздействием этих факторов, в частности, объясняют противоестественное самоубийство 29 американских высококвалифицированных программистов.

Кроме того, длительное (в течение многих лет) воздействие низкоэнергетических СВЧ-излучений способно вызвать существенное

снижение и даже полное подавление иммунитета, что может привести к широкому распространению различных болезней, эпидемий и вымиранию больших масс населения.

Значительный практический интерес представляют исследования по использованию энергоинформационных воздействий при проведении миротворческих операций в зонах региональных военных конфликтов. По оценкам американских специалистов, энергоинформационные воздействия могут значительно снизить активность военных действий, уменьшить число убитых и раненых, а также повысить результативность усилий сторон по мирному урегулированию конфликта[4]. Предполагается, что механизм такого воздействия заключается в том, что в зоне региональных конфликтов создают модулированное магнитное поле с величиной модулирующего сигнала, соответствующей уровню сигналов магнитоэнцефалограммы.

Наиболее эффективно задача информационного воздействия решается с помощью космических средств.

Космические системы могут быть использованы для облучения наземных и воздушных объектов с достаточно большой мощностью. Это может быть использовано для запуска в различных системах управления и связи машинных вирусов, в том числе так называемых дремлющих, которые заблаговременно внедряются в ЭВМ и активизируются по команде.

Энергоинформационные воздействия, в том числе производимые со спутников, опасны тем, что инициируют процессы, энергетика которых на много порядков превышает энергию информационного сообщения. Путем целенаправленного энергоинформационного воздействия могут быть задействованы роботы, начиненные взрывчаткой, приведены в боевую готовность системы ПВО и ПРО, поднята в воздух авиация и т.д.

Таким образом, можно прогнозировать возможность использования спутниковых и других космических систем для энергоинформационных воздействий в качестве информационного оружия. Создание глобальной системы управления поведением людей в любом регионе, городе, местности даст агрессору локальное и глобальное превосходство в решении задач всемирного значения и масштаба и откроет двери к мировому господству.

[4] Eileem M. Walling High Power Microwaves Strategic and operational Implications for Warfare. Air University. Maxwell Air Force Base, May 2000.

Следует, однако, заметить, что достоверная информация о технологиях и процессах скрытого информационного воздействия на большие массы людей практически отсутствует. Известно, что работы в этом направлении велись практически во всех развитых зарубежных странах. Можно также считать доказанной возможность в определенных условиях влиять на психическое состояние больших групп людей (в ходе сеансов гипноза, например) дистанционно с помощью речи, изображений и т.п. Все публикации в этой области ссылаются на существование такого оружия, получившего название «психотронное оружие».

Способы боевого применения информационного оружия

Под способами применения «информационного оружия» в данном случае понимается избранный порядок использования соответствующих средств и сил для достижения поставленных целей с учетом специфики и условий решения задач информационной войны.

Аналитиками выделяются семь факторов, способствующих использованию информационного оружия, которые отличают его от других средств ведения военных действий. Эти характерные черты определяют основные направления проведения исследований способов боевого применения информационного оружия.

Свобода доступа к информационным системам. Развитие информационных сетей и быстрое разрастание и усложнение информационных инфраструктур приводит к появлению новых видов уязвимости от воздействия информационного оружия. В такой среде у компетентного злоумышленника появляется потенциальная возможность практически мгновенного доступа к целому ряду национальных «стратегических целей», входящих в глобальную информационную инфраструктуру. В этих условиях многие разветвленные и сопряженные между собой информационные сети могут стать объектом воздействия со стороны самых разнообразных источников, в том числе обладающих достаточной квалификацией отдельных лиц, негосударственных структур, таких как международные криминальные организации, а также государств, располагающих хорошо подготовленными кадрами специалистов по проведению боевых операций в киберпространстве.

Размытость традиционных границ. Одной из наиболее существенных особенностей развития глобальной информационной инфраструктуры (и

сопряженных с ней национальных инфраструктур) является стирание четких географических границ, традиционно связанных с национальной безопасностью. Так, например, границы, являющиеся атрибутом суверенного государства, становятся все более размытыми. В отличие от последствий, связанных с утратой государством контроля над существующими глобальными финансовым и валютным рынками, усиление взаимосвязи национальной информационной структуры и глобального киберпространства неизбежно ведет к подрыву национального суверенитета. Одним из наиболее серьезных аспектов явления «размытости границ» становится невозможность какого-то четкого различия между внутренними и внешними источниками угроз для безопасности страны. Другой особенностью явления размытости границ в большинстве случаев может стать стирание различий между разными формами действий против государства — от обычной преступности до военных операций. Без четкого разделения источников действий по географическому признаку на внутренние и внешние повышается вероятность того, что будет весьма затруднительно распознавать, имеет ли место традиционный шпионаж, уголовное преступление или «акт войны».

В условиях, когда открывается возможность нанести удар по инфраструктуре страны через киберпространство, у государств, уступающих в обычных средствах военного и экономического влияния, может появиться желание использовать отдельных лиц и/или международные криминальные структуры для проведения «стратегических криминальных операций». В таких случаях определить действительного «зачинщика», отдавшего приказ на проведение акции, будет весьма затруднительно. Последствием подобной размытости границ может стать ситуация, когда страна, подвергаясь удару информационного оружия, не сможет определить суть происходящего. Точно также не сразу будет понятно, какие ответные действия следует предпринять.

Возможность управления восприятием. В процессе развития киберпространства, снижения затрат на доступ к информации и размывания границ национального суверенитета у государственных и негосударственных структур появляется все больше возможностей манипулировать информацией, что является ключевым элементом формирования восприятия. Например, сеть интернет является фактически средством распространения «пропагандистских» материалов из самых разных источников информации. Группы политического толка и неправительственные организации смогут использовать сеть интернет для мобилизации политической поддержки.

Существует возможность, что «факты» того или иного события будут серьезно искажены посредством текстовых, звуковых и видеоинформационных приемов. Такие методы могут позволить широкому кругу заинтересованных лиц или групп реализовать сложный процесс регулирования общественного восприятия или организовать крупные пропагандистские кампании для подрыва доверия граждан к конкретному курсу, проводимому правительством страны. Кампании подобного рода ставят серьезные проблемы не только перед правительством, но также и перед СМИ, призванными быть источником объективных сведений. Прямым следствием этой особенности применения информационного оружия является то, что высшее руководство страны, равно как и общество в целом, могут не знать, что же происходит в действительности.

Нехватка стратегической разведывательной информации. В условиях размытости традиционных границ и свободного доступа в информационные сети разведывательные службы сталкиваются с большими трудностями в обеспечении национального военно-политического руководства достоверной и своевременной стратегической разведывательной информацией относительно настоящих и перспективных угроз информационной войны. Определение объектов разведки становится гораздо более трудной задачей. Классический геостратегический подход сосредоточения разведывательных усилий на конкретном государстве-источнике «угрозы» себя изживает. Объектами разведки становятся транснациональные неправительственные и международные криминальные организации, а также структуры, не являющиеся государственными образованиями. Вес и значимость информационной угрозы будут зависеть от оценки как возможностей и намерений потенциальных противников в киберпространстве, так и от уязвимости конкретных объектов удара.

Определение возможностей того или иного нападающего с помощью информационного оружия затрудняется динамичностью самой природы телекоммуникационных средств киберпространства, используемыми аппаратными и программными средствами и методами защиты информации (например, кодированием). Предполагаемая национальная информационная инфраструктура будет включать набор самых разнообразных компонентов технологически и экономически развитого общества. Такими компонентами могут быть:

- коммутационные системы общего назначения;
- системы управления нефте- и газопроводов;
- сетевые системы энергоснабжения;

- системы управления транспортом;
- система обслуживания федеральных резервных фондов;
- различные системы обеспечения банковских операций;
- система здравоохранения.

Некоторые из показателей уязвимости этих элементов инфраструктуры хорошо изучены, однако многие из них до сих пор еще не исследовались. Для разведывательного сообщества будет чрезвычайно трудным делом разработать и контролировать фиксированный перечень потенциальных угроз. Вследствие проблем с решением задач стратегической разведки страна может так и не узнать, кто будет ее противником, каковы его намерения и возможности в области информационного оружия.

Необычайная сложность задач тактического предупреждения и оценки ущерба. В связи со сложностью ведения стратегической разведки временные ограничения в кризисной обстановке в условиях применения информационного оружия делают тактическое предупреждение и оценку ущерба еще более трудно выполнимой задачей. Существует реальная возможность того, что представленные национальному военно-политическому руководству оценки правоохранительных органов и разведывательных служб по конкретным случаям воздействия или ситуациям будут довольно противоречивы.

Нападающая сторона, используя информационное оружие, способна с беспрецедентной оперативностью проводить стратегические операции и после выполнения задач мгновенно возвращаться в установленные пределы киберпространства. Кроме того, усложнение средств связи, систем управления базами данных и операционных систем, приводит к тому, что некоторые происшествия, внешне схожие с применением средств информационной войны, будут лишь следствием неблагоприятного стечения обстоятельств или конструктивных недоработок.

Не исключается также возможность проведения стратегических наступательных мероприятий, в ходе которых на протяжении многолетней заблаговременной «подготовки поля боя» осуществляется скрытое внедрение в систему соответствующих средств, в нужный момент обеспечивающих ее выведение из строя. Такие мероприятия во многих случаях могут быть диагностированы неправильно. Следствием указанных выше особенностей может стать ситуация, когда страны окажутся в полном неведении о том, что «удар» с помощью

информационного оружия уже наносится, кто его наносит и каким способом.

Трудность создания и сохранения коалиций. Неизбежно столкновение с тем, что формирование и сохранение коалиций государств для совместных решительных действий в будущем против военной угрозы явится необычайно сложной задачей, которая к тому же будет существенно усложнена вследствие проблем, обусловленных возможностями информационного оружия. Многие союзники сами по себе могут быть очень уязвимы от подобных средств вооруженной борьбы в случае воздействия на их ключевые инфраструктуры. Некоторые факторы усугубляют эту проблему.

Во-первых, главные члены коалиции и/или дружественные страны столкнутся с той же тяжелой проблемой организации надежной стратегической разведки и обеспечения тактического предупреждения и оценки ущерба. С началом применения информационного оружия, прочность коалиции подвергнется большому испытанию, поскольку все союзники окунутся в информационный «туман». Могут также возникнуть острые проблемы с реализацией коалиционных планов, если один из партнеров окажется менее защищенным от информационного оружия.

Во-вторых, многие страны остаются значительно уязвимыми в ключевых сферах экономики (например, в области связи, энергетики, транспорта и финансов), которые могут стать объектом удара противника в попытке подорвать коалиционное единство. Особенно уязвимыми могут оказаться новые системы, приобретенные за рубежом в интересах быстрого и целесообразного по критерию «стоимость-эффективность» коммерческого внедрения. В будущем зависимость от союзников и партнеров по коалиции, которые потенциально являются уязвимыми от информационного оружия, окажет существенное влияние на стратегию национальной безопасности и будет предполагать оказание им со стороны более продвинутых в этом вопросе стран своевременной и солидной помощи и поддержки.

Можно сделать главный вывод, что применение информационного оружия приводит к высокой неопределенности в выявлении факта его применения, идентификации противника и оценки ущерба. Кроме того, при двустороннем вооруженном конфликте совершенно непредсказуемой является и реакция стороны, подвергшейся воздействию информационного оружия. Может сложиться ситуация, когда выявление

факта применения информационного оружия даже в очень ограниченном масштабе может привести к «испугу» и предположению, что вскрыта только «вершина айсберга» информационной атаки. Вслед за таким выводом может последовать ограниченное или массированное применение ядерного оружия.

Принципы применения информационного оружия

Общие принципы применения информационного оружия состоят в следующем:

- главными объектами поражения с помощью информационного оружия являются системы управления, связи и аппарат принятия решений противника;
- первоочередному подавлению или уничтожению подлежат все находящиеся у противника информационно-разведывательные средства еще до начала широкомасштабных боевых действий;
- до потребителей должен доводиться максимально возможный объем информации; разведывательная информация должна доводиться непосредственно до потребителей на поле боя, а не через промежуточные командные инстанции;
- безусловному использованию в любых конфликтах подлежат все возможные средства воздействия на информационную инфраструктуру; необходимо опередить противника в переносе борьбы на уровень информационного противоборства; при этом промедление опасно, т.к. силы противника могут оказаться недооцененными;
- все усилия при организации и применении информационного оружия должны быть полномасштабными и всеобъемлющими по характеру, но быть вне контроля на оперативно-тактическом уровне со стороны политиков, которые должны только принять решение на проведение подобных операций.

Следует отметить, что информационное оружие окажет огромное воздействие на характер проведения военных операций в ближайшем будущем и может даже превратить всю военную кампанию в одну большую информационную наступательную операцию.

Например, перед началом военных действий может ставиться задача завоевания превосходства в информационном пространстве подобно тому, как в настоящее время успех кампании (операции) в значительной степени связывают с завоеванием господства в воздухе и на море. Результатом информационного превосходства явится то, что все пространство театра войны становится как бы «прозрачным и видимым»

для своих войск и делается «туманным» для противника. Растянутый по времени «импульс информационного удара», некоторое подобие которого можно было наблюдать в ходе операций в Панаме, в войне в Персидском заливе и который четко просматривается в боевых действиях против Югославии, должен ошеломить противника, лишив его всякой возможности адекватного противодействия. При этом конечная цель кампании должна быть достигнута в случае успеха быстро и решительно с минимальными потерями материальных и людских ресурсов.

В настоящее время наиболее отработанной концепцией применения информационного оружия можно считать концепцию борьбы с системами боевого управления ВС США. Выдвинутая в начале 90-х годов одновременно с началом формирования военной и национальной информационной инфраструктуры концепция борьбы с системами боевого управления, предполагает осуществление в ходе ведения боевых действий целенаправленного согласованного по задачам, месту, времени и объектам комплекса мероприятий по дезорганизации, подавлению и уничтожению систем и средств управления войсками и оружием противника.

В ходе локальных конфликтов, на учениях, а также в ходе аналитических расчетов и моделирования была неоднократно продемонстрирована высокая эффективность мероприятий борьбы с системами боевого управления (по оценкам американских специалистов, дезорганизация системы боевого управления равнозначна снижению боевого потенциала группировки на 50% и более, что в ряде случаев делает соотношение сил сторон несоизмеримым)[5].

Главным элементом борьбы с системами боевого управления является комплексное воздействие (огневыми, радиоэлектронными и иными средствами) на системы и средства управления с целью их физического уничтожения, выведения из строя или подавления помехами. Организация такого воздействия предполагает обнаружение средствами радио- и радиотехнической разведки радиоэлектронных систем управления, определение их местоположения, выявление предназначения и роли в системе управления войсками и наведение на них средств поражения и подавления.

[5] Информационная война и борьба с системами боевого управления. Инструкция Начальника штаба ВМС США 3430.25, 1999.

Воздействие на военные средства связи систем управления может оказываться следующими основными способами:

- поражение обычными боеприпасами по целеуказаниям средств радио- и радиотехнической разведки;
- поражение высокоточными боеприпасами по данным средств радио- и радиотехнической разведки, уточненным другими средствами разведки, с точным целеуказанием и частичным самонаведением на конечном участке;
- поражение высокоточными боеприпасами нового поколения интеллектуальными боеприпасами, выводимыми в район местонахождения цели по данным радио- и радиотехнической разведки с последующим самостоятельным поиском цели и самонаведением на ее уязвимые элементы;
- радиолокационное подавление средств связи маскирующими помехами;
- создание имитирующих помех, затрудняющих вхождение в связь, синхронизацию в каналах передачи данных, инициирующих функции повторных запросов и дублирования сообщений;
- подавление с помощью средств силового радиоэлектронного подавления (мощного электромагнитного излучения, создающего подавляющие помехи за счет паразитных каналов приема);
- выведение из строя радиоэлектронных компонентов за счет воздействия больших уровней электромагнитных или ионизирующих излучений;
- нарушение свойств среды распространения радиоволн (например, срыв коротковолновой радиосвязи за счет модификации параметров ионосферы).

Способы боевого применения информационного оружия на основе программных кодов определяются двумя факторами:

- воздействие на ресурсы системы оказывается извне системы через устройства ее сопряжения с системой, имеющей упрощенный доступ для вероятного противника;
- воздействие на ресурсы системы оказывается изнутри системы, лицами, имеющими права на отдельные виды ее администрирования.

В первом случае возможность использования информационных технологий для проведения информационной наступательной операции определяется наличием средств доступа к системе, которого скорее всего может и не быть, и проработанности политики компьютерной безопасности на самом объекте воздействия. Существует мнение, что в

случае реального конфликта наиболее критические элементы инфраструктуры вооруженных сил и государства в целом будут изолироваться от общедоступных систем типа глобальной информационной системы интернет. Кроме того, в частности в США, прорабатываются вопросы отключения в подобных случаях даже систем союзников от своих информационных систем. Однако в случае развертывания многонациональных формирований возможности использования информационных технологий для ведения информационной наступательной операции возрастают.

Использование информационных технологий в информационной наступательной операции наиболее эффективно в случае воздействия на ресурсы системы изнутри. При этом, в зависимости от полномочий лица, осуществляющего воздействие, результатом может быть полный выход информационной системы из строя на продолжительный период времени. Следует иметь в виду, что понятие «продолжительный период времени» соотносит время неработоспособности системы с промежутком времени, на котором реально возникновение «информационного превосходства», т.е. необходимо обеспечить неработоспособность системы в строго определенные моменты времени. Для проведения подобного воздействия может использоваться как завербованный персонал, так и внедренные ранее программные закладки или компьютерные вирусы, активизирующиеся в определенный момент времени или при возникновении определенной ситуации (появлении определенных признаков).

Способы применения информационного оружия определяются также целью воздействия. Наиболее общие цели могут заключаться в выведении из строя в заданном районе всей радиоэлектроники или снижении эффективности функционирования отдельных подсистем систем управления войсками и оружием (отдельных видов и типов датчиков, подсистемы передачи информации, подсистемы хранения информации, подсистемы целеуказания, подсистем управления воздушным движением, метеообеспечения, сигналов точного времени и т.д.)

Воздействие может оказываться как на программное и аппаратное обеспечение, так и на информационный ресурс, а также обеспечивающие системы: электропитания, охлаждения и др. В систему может быть введена ложная информация, например за счет использования средств имитации голоса для дезинформации операторов или несанкционированного ввода данных или сообщений. В системе может

быть нарушена адресация сообщений либо искусственно вызвана перегрузка отдельных элементов системы.

Следует отметить также, что эффективность применения информационного оружия тесно связана с задачами комплексного разведывательного и контрразведывательного обеспечения. Разведывательное обеспечение в этом случае должно включать:

- создание баз данных и накопление детальной информации об обстановке в районах потенциальных конфликтов;
- выявление ключевых узлов и элементов в системах управления, линиях связи, коммуникаций и в приемных центрах стран-потенциальных противников. На основе этого анализа должен быть составлен общий перечень объектов с подробным описанием основных целей, а также критические временные параметры работы для конкретных элементов систем управления. Чрезвычайно важным является знание порядка функционирования систем и средств управления и связи потенциального противника как в обычной обстановке, так и в начальный период войны, организационной структуры частей и подразделений связи, их деятельности и планов мобилизационного развертывания. Эти данные должны с достаточной степенью детализироваться и обеспечивать эффективное применение высокоточных средств поражения и средств радиоэлектронной борьбы;
- оценку возможностей и слабых мест потенциальных объектов поражения в системе управления и связи. Эта информация позволяет на этапе планирования определять в качестве целей те элементы системы управления и связи противника, вывод из строя которых (путем нарушения режима работы, дезинформации, физического уничтожения или демаскировки) в максимальной степени облегчит выполнение боевых задач;
- выявление основных политических и военных деятелей в странах потенциального противника. Работа как с формальными, так и с неформальными силовыми структурами. Сбор биографических данных и, по возможности, психологических характеристик на лидеров для обеспечения (как минимум) мероприятий по воздействию на них методами психологической борьбы;
- анализ возможностей противника по воздействию на системы управления и связи. Сбор точной информации и классификация всех источников радиоизлучения во всем диапазоне электромагнитного спектра;
- обеспечение своевременной и достоверной информацией о возможности внезапного нападения противника. Своевременное

информирование должностных лиц в ходе о текущем состоянии, возможностях и вероятных действиях противника.

Можно представить, например, такой вариант применения информационного оружия в крупном региональном конфликте.

В период обострения обстановки проводится широкий спектр мероприятий информационной войны. Выявляются критические элементы информационных систем противника, отрабатываются способы воздействия на них, блокируется выход на внешние информационные системы, проводятся скрытые мероприятия по дезорганизации кредитно-денежного обращения, население подвергается массированной психологической обработке.

За несколько часов до начала боевых действий проводится решительное «информационное наступление»: дезорганизуются системы управления телекоммуникациями, энергоснабжением, транспортом, подавляется работа компьютерных систем государственных органов и вооруженных сил.

Степень подавления строго дозируется с тем, чтобы избежать возможного в обстановке всеобщего хаоса неконтролируемого развития событий. Широкий масштаб принимают мероприятия по дезинформации.

Целью проводимого информационного наступления является рефлексивное управление действиями противника, при котором его реакция является вынужденной, предсказуемой и выгодной для своей стороны.

Непосредственно перед началом воздушной фазы операции (воздушной кампании) средствами радиоэлектронной борьбы дезорганизуется и подавляется система управления войсками и оружием противника, чем демонстрируется его беззащитность перед лицом ударов авиации и наземного высокоточного оружия.

В момент пролета авиации с обычным и информационным оружием средства ПВО дополнительно выводятся из строя с помощью компьютерных вирусов и активизации специальных «закладок».

Высокоточным оружием нового поколения уничтожаются антенные системы сохранивших работоспособность РЛС и объекты энергоснабжения, поражаются ключевые элементы инфраструктуры. С

помощью неядерных генераторов электромагнитных импульсов выводится из строя радиоэлектронная и электротехническая аппаратура, а также ЭВМ.

Заблаговременно перед началом боевых действий агентурными и другими методами осуществляется проникновение в компьютерные сети и базы данных, вносятся культуры микроорганизмов, разъедающих радиоэлектронные компоненты. На заключительной стадии крупного регионального конфликта применение информационного оружия аналогично его использованию в миротворческих операциях. Проведенные оценки показывают, что применение информационного оружия должно постоянно сопровождаться ограниченным применением обычного оружия, особенно высокоточного, или угрозой его применения.

Другим важным условием успешного применения информационного оружия является решение вопросов надежной защиты своих вооруженных сил как от информационного, так и от обычного оружия, поскольку концепция ведения информационной войны предполагает его использование только при малом или сверхмалом уровне собственных потерь. Эти вопросы, например в США, решаются комплексно путем повышения эффективности индивидуальных средств защиты и защищенности боевой техники, использования робототехнических устройств, увеличения дальности и информативности средств разведки.

Некоторые примеры применения информационного оружия

Отдельные виды информационного оружия (средств ведения информационного противоборства): радиоэлектронные, программно-аппаратные средства, средства морально-психологического воздействия применялись в вооруженных конфликтах последнего десятилетия с участием американских войск, в том числе в Панаме в 1989 г., в Ираке в 1991 г., на Гаити в 1994 г. и в Боснии в 1997 г.

Информационное оружие, предназначенное для вывода из строя электросетей впервые было применено ВВС США в Ираке, а затем и в Югославии. В качестве носителей этих средств использовались крылатые ракеты и управляемые авиационные кассеты.

Так, в операции многонациональных вооруженных сил в зоне Персидского залива против Ирака «Буря в пустыне» в 1991 г. использовались средства

радиоэлектронного подавления и радиоэлектронной разведки в стратегическом, оперативном и тактическом масштабе. В группировке сил и средств радиоэлектронной борьбы войск коалиции имелись наземные станции помех и комплексы помех, размещенные на вертолетах и самолетах, позволявшие решать задачи радиоэлектронного подавления линий связи иракских войск, радиолокационных станций и средств, систем противовоздушной обороны Ирака.

Во время войны в Персидском заливе впервые были применены крылатые ракеты «Томогавк», боевая часть которых снаряжалась небольшими катушками с намотанными на них нитями из углеродных волокон. Использование таких боевых частей приводило к срабатыванию автоматов защиты электроэнергетических систем, что позволило американцам вывести из строя до 85% системы электроснабжения Ирака.

Специализированный боеприпас BLU-114/B, предназначенный для вывода из строя энергетической (электросети, трансформаторы, электростанции и т.п.) инфраструктуры, был применен в Сербии 2 и 7 мая 1999 г. с самолетов F-117A. Он состоит из большого количества углеродных волокон толщиной в десятые доли миллиметра и графитового порошка, упакованных в небольшой контейнер. Такими боеприпасами оснащались неуправляемые авиационные кассеты, точность наведения которых составляет более 100 м.

После раскрытия кассеты и разбрасывания суббоеприпасов BLU-114/B над целью содержимое контейнеров образует плотное облако, дрейфующее в воздухе. При контакте облака с трансформатором или другим электрооборудованием, находящимся под высоким напряжением, происходит короткое замыкание и образуется электрическая дуга. Порошок графита, являющийся хорошим проводником электрического тока, увеличивает площадь поражения и усиливает эффект воздействия. Если сила тока в дуге достаточно большая, то она может вызвать разрушение оборудования или пожар.

После использования этого оружия авиационная кассета SUU-66/B получила название «Выключатель электричества».

В войне против Ирака американцами активно использовались забрасываемые радиопередатчики помех. Широкое применение нашли и дистанционно-пилотируемые летательные аппараты-постановщики помех.

Для быстрого подавления иракской ПВО была создана сложная помеховая обстановка за счет применения имитирующих многократных и однократных помех, маскирующих помех, ответных шумовых помех с согласующим спектром, прицельных и заградительных помех, мерцающих помех и т.д. Активные помехи ставились во всех диапазонах частот, в которых могли работать средства связи иракских войск и иракские радиолокационные станции ПВО.

По оценке всех специалистов, радиоэлектронная борьба в операции «Буря в пустыне» носила плановый и комплексный характер. Ее целями являлось создание благоприятных условий для внезапного использования авиации, сухопутных войск и высокоточного оружия, а также — обеспечение в целом превосходства в управлении.

Отмечалось, что в нарушении и блокировании системы ПВО Ирака сыграло свою роль использование программно-аппаратных «закладок», внедренных в компьютеры, приобретенные военным ведомством Ирака у зарубежных фирм. Эти «закладки» были активизированы по специальному сигналу, поданному извне, и нарушали нормальную работу систем управления ВС Ирака в моменты боевых действий.

В печати сообщалось, что французские спецслужбы, используя наличие «изначальных закладок» в программном обеспечении истребителей «Мираж» иракской армии, по кодовому сигналу отключили бортовые компьютеры этих самолетов, и они не смогли принять участие в боевых действиях.

История войн и вооруженных конфликтов свидетельствует, что важной составной частью военной и политической борьбы являлось психологическое воздействие. Однако только в XX веке эта деятельность приобрела действительно научно обоснованный характер и стала опираться на достижения общей, социальной, политической, этнической психологии, психиатрии, политологии, военной истории, филологии, психолингвистики и других наук из области естествознания.

Поворотным пунктом в развитии теории и практики психологического воздействия в условиях боевой обстановки стала первая мировая война. Этот этап характеризовался широкомасштабным развитием средств изготовления и доставки пропагандистских материалов, распространением грамотности среди населения стран, принимавших участие в войне, возникновением специальных государственных органов

для ведения пропаганды. Ее основной формой стала печатная пропаганда (листовки, газеты, брошюры, письма пленных, открытки, плакаты и т.д.).

Накопленный в этот период опыт позволил специалистам сделать важный вывод, оказавший в дальнейшем большое влияние на моделирование процесса психологического воздействия: успешным оказывается воздействие, направленное на подрыв морального духа противника путем его информирования о наиболее злободневных темах, воздействующих на обыденное сознание военнослужащего.

Целью проводимых психологических мероприятий в большинстве случаев являлось инициирование панических настроений и внушение страха путем прямого насилия или эксплуатации его последствий. Такая концепция информационной войны была разработана на основе теоретического положения, согласно которому эффективность психологического воздействия определяется силой и глубиной депрессии противника, вызванной деморализующим воздействием оружия в сочетании с подрывной пропагандой.

Инновационные психотехнологии были широко использованы США для моделирования процесса психологического воздействия во время войны в Персидском заливе. В материалах пропагандистского характера, отличавшихся доходчивостью и простотой, широко использовались особенности национальной психологии населения Ирака. При их подготовке применялись традиционные исламские иллюстрации и орнамент, изречения из Корана, а также цвета, наиболее характерные для мусульманской культуры. В радиопрограммах звучала сентиментальная арабская музыка, передачи вели дикторы, в совершенстве владеющие местными диалектами. Эти меры способствовали формированию доверительного отношения к информационным материалам, их принятию и осмыслению.

Широкое применение в информационной войне для психологического воздействия на мировое сообщество нашла так называемая «сувенирная пропаганда». Во многих странах мира в продажу поступали товары с антииракской символикой, в частности туалетная бумага с портретами С. Хусейна, майки с изображением летящих ракет и соответствующими надписями — «Привет от морской пехоты США», «До встречи в Багдаде» и пр.

Кроме того, была введена жесткая цензура на информацию, поступающую по каналам СМИ из зоны боевых действий.

Круглосуточные передачи СМИ в прямом эфире, создававшие иллюзию объективности и беспристрастности в освещении происходящего, хотя на самом деле они были частью хорошо продуманной стратегической дезинформации.

Следует отметить, что в формах и методах психологического воздействия, применяемых специальным аппаратом армии США в других вооруженных конфликтах второй половины XX века сохранялась определенная преемственность. Основной упор постоянно делался на внушение страха, подавление способности к сопротивлению, формирование глубокой психологической депрессии, нанесение психических травм с использованием всего арсенала боевых и небоевых средств.

Трансляция с воздуха радиовещательных и телевизионных программ, подготовленных американскими специалистами по психологическим операциям, осуществлялась в рамках комплекса мероприятий, включавшего также операции по радиоэлектронному подавлению военных систем связи и управления, гражданских вещательных станций. На самолетах, обеспечивавших эти мероприятия, были установлены радиопередатчики для излучения сигналов коротковолнового и ультракоротковолнового диапазонов, а также для телевизионного вещания в метровом и дециметровом диапазонах.

По оценке специалистов Гарвардского университета, среди приоритетов по «вкладу» видов оружия в разгром иракских войск первое место отводилось средствам и системам «информационных операций»[6].

Мероприятия по психологическому воздействию на противника проводились в Панаме — в 1989 г., на Гаити — в 1994 г., в Боснии — в 1997 г.

На Гаити специалисты одного из подразделений психологических операций сухопутных войск США на основе предварительно проведенных исследований разделили население острова на 20 групп и вели целенаправленную психологическую обработку каждой из них. Перед вторжением на Гаити ЦРУ, в частности, организовало анонимные звонки по телефону гаитянским военнослужащим с предложениями сдаться в плен, а также направило угрожающие послания по компьютерным сетям членам правительства.

[6] Test and Evaluation of Defense Information Systems, Information Warfare, Information Assurance. NDIA 15th Annual Test and Evaluation Conference. Nevada, 8-11 March 1999.

В 1997 г. в Боснию и Герцеговину была направлена группа самолетов для подавления радио- и телепередач Сербской Республики в период выборов в местные органы власти и трансляции собственных сообщений о деятельности сил по стабилизации.

Наиболее распространенным применением средств, относимых к информационному оружию, все-таки является криминальная и террористическая деятельность. Примеры криминального проникновения или воздействия на информационные системы исчисляются уже сотнями тысяч. Лидируя в производстве и применении средств обработки информации, США стали безусловным лидером и в информационно-криминальной сфере.

В СМИ имеются факты применения информационного оружия в гражданской сфере с целью: просмотра, копирования, хищения в корыстных целях, изменения или уничтожения информации, находящейся в компьютерных и телекоммуникационных сетях, банках данных и базах знаний, хищения системного и прикладного программного обеспечения, информационной блокады (информационного давления) и других видов компьютерных злоупотреблений. Ранее в тексте уже приводился целый ряд примеров криминального использования информационных средств. Здесь нет смысла останавливаться на них подробно. Но дополнительного внимания все-таки требует международный характер информационной преступности, что явилось прямым следствием свойства трансграничности информационного оружия.

В настоящее время известно свыше 100 типов атак на компьютерные системы с применением информационного оружия. Количество вторжений год от года практически удваивается, несмотря на использование все более совершенных защитных систем, поскольку компьютерные злоумышленники применяют весьма изощренные методы и высокоэффективную аппаратуру.

Одними из основных объектов проникновения «компьютерных» взломщиков являются банковские компьютерные сети, из которых похищаются значительные денежные суммы. Но объектами атак стали военные, научные и даже энергетические центры.

В 1987-1989 гг. западногерманские хакеры атаковали компьютерные системы Пентагона, НАСА, исследовательских организаций Лаборатории Лоуренс Беркли и Лос-Аламосской национальной лаборатории, вызвав большие потери секретной информации.

Хакер из Чикаго Г. Зин в 1987 г. открыл доступ к файлам системы управления ракетами на базе ВВС США «Роббинс». Его вторжение обнаружили после того, как он снял копии программного обеспечения, оцениваемого в 1,2 млн долл. США, включая программы искусственного интеллекта, которые считались сверхсекретными.

В 1988 г. Р.Т. Моррис из Корнеллского университета (США) в экспериментальных целях создал программу (вирус или «червь» Морриса), способную распространяться и самопроизвольно размножаться в сетях ЭВМ, минуя средства обеспечения безопасности. В результате программа вышла из-под контроля ее создателя и поразила свыше 6000 компьютеров сети интернет. Из-за вирусной атаки часть сетей в составе интернет вышла из строя на срок до пяти суток. Общие затраты, связанные с ликвидацией последствий вируса Морриса, составили свыше 98 млн долл. США. Ущерб был бы гораздо больше, если бы вирус имел целенаправленный разрушительный характер.

В 1989 г. от заложенной группой хакеров «Легион оф Дум» «логической бомбы» в компьютерную систему американской компании АТТ был нанесен ущерб в один миллион долларов США. В том же году эта группа произвела разрушения в информационной системе министерства ВВС США, оцениваемый в 25 млн долл. США.

В 1990 г. М. Лаунфербергер внедрил «логическую бомбу» в программу «Атлас Миссайл» американской компании «Дженерал Динамик Спейс Дивижион».

В 1990 г. проникновение группы австралийских хакеров в американские информационные системы НАСА, Национальную лабораторию Лоренс Ливермор и Исследовательскую лабораторию военно-морских сил США вызвало остановку работы агентства НАСА на 24 часа.

Фиксировались нападения на компьютерные сети практически всех государственных учреждений. Только по подсчетам Пентагона, его компьютерные сети «взламываются» примерно 250 тыс. раз в год, при этом не менее 500 раз это серьезные попытки проникновения в секретные системы. По оценке руководителя подразделения информационных операций ВМС США Дж. Ньюмана, высказанной им в интервью радиостанции «Немецкая волна»[7], компьютерные сети ВМС США

[7] 19 июля 1999.

подвергаются атакам 12 тыс. раз в год, правда лишь 0,5% из них достигают успеха. Разного рода преступлений только в 1998 г. и только в США зарегистрировано (то есть принято к уголовному рассмотрению) свыше 300[8].

Имеются сведения об атаках на информационные системы (следующей мишенью могут быть системы управления) ядерных центров. В 1998 г. такой атаки подвергся индийский Центр ядерных исследований им. Хоми Бабы.

Конечно, американцы не единственные в этом роде. На территории Западной Европы ежегодно фиксируется до 300 удачных проникновений хакеров в военные, государственные и коммерческие сети.

Известны нападения на информационные сети Китая, Тайваня, Индии, Индонезии. Идет прямое информационное противоборство Пекина и Тайбэя[9], противостояние хакерских групп Армении и Азербайджана[10]. Размеров войны достигла борьба хакеров США и Китая после конфликта с американским самолетом разведчиком, задержанным Пекином в мае 2001 г. И, отметим, победа в этой войне оказалась не на стороне признанного компьютерного лидера.

Не обошла сия чаша и Россию. Только один пример: 12 февраля 2000 г. произошло, пусть не столь масштабное, но качественно весьма значительное проникновение в один из самых крупных российских серверов «Росбизнесконсалтинг». Взломав защиту, хакер от имени чеченских националистов поместил доступное всем клиентам обращение, содержащее призывы к физическому устранению В.В. Путина как основного виновника произошедших на Северном Кавказе событий.

Имеются примеры использования информационных воздействий в политических целях. Восточный Тимор. Сразу после референдума о независимости этой провинции Индонезии общественная организация «Ист Тимор Компани» провела с территорий Испании, Португалии и Франции атаку на государственные интернетовские сайты Индонезии. Поражены веб-страницы, принадлежащие правительственным организациям Индонезии, созданы и внедрены новые компьютерные вирусы, специально предназначенные для поражения индонезийских

[8] *Computer Weekly*, 15 April 1999, p.30.
[9] Модестов С.А. Незримая война обостряется. *Независимое Военное Обозрение*, №3, 2000.
[10] *Итар-Тасс*, 14 февраля 2000.

информационных объектов. Эти информационные операции, проведенные, отметим вторично, с территории Европы (вот пример «трансграничности» информационного оружия), явились примером прямого применения информационного оружия для решения конкретных внутриполитических задач.

Более чем представительный список ставших известными кибератак показывает, что такие средства и методы уже освоены и международными террористическими и экстремистскими организациями (в том числе такими, как Аум синрике, Хамаз, группировки бин Ладена и Тупек Амару) и национальными сепаратистскими движениями, такими как индонезийское движение за отделение Восточного Тимора («Ист Тимор Компани»), «Тигры освобождения Тамил Илама» и др.

Таким образом, можно констатировать, что практически все виды информационного оружия уже реально испытаны и взяты на вооружение как армиями, так и преступным миром.

ГЛАВА 4. ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО — НЕВИДИМАЯ ВОЙНА В МИРНОЕ ВРЕМЯ

Приведенные в конце предыдущего раздела примеры показывают, что средства информационной борьбы могут применяться не только для обеспечения собственно боевых операций, но и в качестве самостоятельных действий, имеющих свой, присущий только им, характер. Поэтому, в данном случае правильно было бы говорить не об «информационной войне», а об «информационном противоборстве».

Последствия информационного воздействия могут оказаться сопоставимыми с последствиями боевых действий в рамках традиционного военного противоборства. Отсюда делается вывод, что говорить об информационном противоборстве следует прежде всего в контексте межгосударственных отношений, а также применительно к террористическим (или квазитеррористическим) организациям, чьи действия затрагивают жизненно важные интересы и прямо направлены против того или иного государства.

Основные направления информационного противоборства

К концу 90-х годов на Западе сформировался целый ряд экспертно-аналитических групп, принадлежащих к различным теоретическим школам и исследующих различные аспекты многофакторной проблемы ведения информационного противоборства. Разрабатываемые теоретические концепции ведения информационного противоборства являются объектом самого серьезного обсуждения в научных кругах и используются при разработке практических шагов по подготовке к ведению информационного противоборства. Естественно, в реальности еще далеко от полного воплощения в жизнь какой-либо из этих разработок, однако использование их отдельных аспектов считается вполне оправданным.

Анализ появляющихся и постоянно уточняемых теоретических построений позволяет выявить общий вектор развития информационного противоборства. Сегодня основное внимание, в отличие от предыдущих лет, уделяется уже не собственно технической стороне проблемы, а организационным и психологическим аспектам информационного противоборства, причем информация сама рассматривается как цель и средство действий, предпринимаемых для разрешения конфликта. Такая

смена приоритетов, естественно, не снимает с повестки дня разработку и совершенствование технических аспектов, поскольку информационные технологии выступают если не первостепенными, то необходимыми компонентами даже в самых футуристических теориях информационного противоборства.

Классифицируя рассмотренные подходы в соответствии с теми объектами, на которые предполагается оказывать целенаправленное информационное воздействие в ходе ведения информационного противоборства, можно выделить следующие четыре основные группы объектов воздействия:

- системы управления и принятия решений (гражданские, военные, социальные, культурные);
- гражданская информационная инфраструктура (системы телекоммуникации, информационные системы транспорта, энергетики, финансов, промышленности);
- военная информационная инфраструктура (системы контроля, управления и связи, разведка);
- системы вооружений.

Логично предположить, что указанные группы могут подвергаться различному воздействию в ходе конкретных информационных операций. Например, компьютерная сеть может быть либо уничтожена или повреждена физически, либо из нее может быть похищена критически важная информация, либо ее программное обеспечение может быть изменено в результате вирусного проникновения или хакерской атаки. Кроме того, информационные системы могут служить средой, в которой ведется противоборство.

Детальный анализ проблемы ведения информационного противоборства, включая определение возможностей для планирования мероприятий по осуществлению или отражению информационного нападения, требует более четкого выявления основных направлений информационного противоборства. Согласно М. Либики[1] (приложившему много усилий для того, чтобы теоретические разработки в этой области нашли свое практическое воплощение), можно выделить семь таких направлений:

1) борьба с системами управления;
2) информационно-разведывательные операции;
3) электронная борьба;

[1] Libicki M. What is Information Warfare? ACIS Paper 3, August 1995.

4) психологическая борьба;
5) «хакерская» борьба;
6) «кибернетическая» и «сетевая» борьба;
7) экономическая информационная борьба.

В последующих разделах приводятся основные характерные черты и особенности указанных направлений информационного противоборства.

Борьба с системами управления

Борьба с системами управления в контексте информационного противоборства может быть определена как военная стратегия (в рамках информационных операций при проведении военных действий), предусматривающая физическое уничтожение таких систем и отсечение командных структур вооруженных сил противника от управляемых частей с целью воспрепятствовать стабильному процессу боевого управления и руководства.

Такого рода борьба с системами управления может достигаться как непосредственным уничтожением управляющих структур (так называемое «обезглавливание»), так и разрушением коммуникаций, связывающих системы управления с подчиненными подразделениями («удушение»). Выбор метода борьбы во многом определяется поставленными тактическими и стратегическими целями.

Обезглавливание

Ликвидация командных структур противника является старым и хорошо испытанным тактическим и стратегическим приемом ведения войны, чему имеются многочисленные примеры в истории. Однако сама возможность поражения и уничтожения командных структур постоянно менялась. Если в прошлом командование для руководства войсками должно само было находиться на поле боя или в непосредственной близости от него, то с появлением технических средств коммуникации (телефония, радиосвязь и т.п.) командование получило возможность располагаться на значительном расстоянии от районов ведения боевых действий.

Еще более важным изменением стало то, что командные структуры по своим масштабам разрослись от относительно компактных штабных структур до целых командных центров, разветвленная внутренняя система которых включает в себя не только объекты командной инфраструктуры и собственно командование, но и развитую

информационную инфраструктуру (оборудование, внутренние и внешние информационные потоки), прямо влияющую на эффективность достижения военных целей.

Грамотно проведенная и надлежащим образом скоординированная информационная атака на такой командный центр способна привести к срыву планов противника даже без физического уничтожения командования. Более того, вопреки общепризнанным недостаткам узконаправленного воздействия на противника, даже изолированная атака на системы контроля и управления может иметь стратегический успех. Это связано с тем, что критическая информация обычно концентрируется в весьма малочисленных и относительно легко выявляемых местах, своего рода «нервных узлах». Такими информационными «нервными» узлами являются непосредственно командные пункты, центры связи, системы энергоснабжения и т.п. Выявление и последующая ликвидация таких узлов может привести к полной потере противником возможности управления задействанными силами.

Физическая атака и уничтожение командных центров не является единственным способом достижения результата поставленной задачи — они могут быть выведены из строя также при обесточивании, электронные системы могут быть разрушены достаточно мощным электромагнитным импульсом, а данные и программное обеспечение — компьютерными вирусами. Однако следует иметь в виду, что эти методы не столь наглядны, как физическое поражение, а их оценка «затрата-эффективность» не может быть столь же легко просчитана, как в случае с обычными вооружениями. Тем не менее, несомненными достоинствами информационного оружия являются сложность обнаружения противником самого факта атаки, а также возможность и максимальная эффективность ее проведения до начала традиционных боевых действий (войны). Вместе с тем, использование «мягкого» оружия потребует большой предварительной работы, связанной с обнаружением ключевых командных центров противника, на которые будет проводиться атака, выявлением их уязвимых мест и, соответственно, тщательным выбором способа атаки.

У противника возникает также проблема защиты командных центров от подобных атак. В случае традиционных боевых действий их безопасность обеспечивается созданием защитных сооружений, повышением мобильности, маскировкой либо совокупностью этих методов. Возможность проведения противником информационной атаки требует,

наряду с этим, учета ряда новых аспектов, требующих повышенного внимания. К ним принято относить:

- максимально возможное снижение рассеянного электромагнитного излучения информационных систем либо генерирование фонового маскирующего излучения;
- обесточивание незадействованных энергетических систем и коммуникаций, связывающих центры управления с внешними системами;
- обязательное дублирование питания информационных систем через независимые генераторы электроэнергии, расположенные на самом командном центре;
- децентрализация информационных сетей, создание замкнутых, невзаимосвязанных функциональных информационных контуров;
- создание минимально необходимой информационной инфраструктуры, состоящей из как можно меньшего набора информационных систем, обеспечивающих устойчивое функционирование систем управления в целом и легко восстановимых в случае их повреждения в результате атаки;
- резервирование информационных систем и создание резервных копий критической информации;
- децентрализация управляющих структур в угрожаемый период, что подразумевает уменьшение личных контактов персонала командного центра, а также возможную отмену крупных совещаний и других встреч, требующих физического присутствия лиц, принимающих решения. Вместо этого предлагается проводить телеконференции и другие подобные мероприятия.

В самом общем виде перечисленные меры могут быть отнесены к трем основным направлениям: децентрализации, уменьшению числа избыточных каналов связи командных центров с внешним миром и созданию дублирующих и резервных систем, которые могут стать целью информационной атаки. Реализация таких мер потребует затраты значительных денежных средств, времени на их разработку и создание, а также существенно усложнит общую архитектуру всей системы командования и боевого управления.

Удушение

Стратегия «удушения», в отличие от «обезглавливания», предусматривает поражение в первую очередь не командных и управляющих центров, а внешних линий связи и, особенно, тех узлов коммуникационной системы, в которых концентрируются потоки критической информации.

Разрушение этих коммуникаций будет означать, что системы управления в целом окажутся неспособными надлежащим образом выполнять свои функции.

В рамках данной стратегии успех атаки в решающей степени зависит от точности определения структуры коммуникационной составляющей системы управления, а также, желательно, и общего построения информационной инфраструктуры противника. Так, США во время проведения операции «Буря в пустыне» смогли парализовать системы государственного управления Ирака, поразив принадлежавшее фирме AT&T здание в центре Багдада. Аналогичные попытки предпринимались и в период войны НАТО против режима Милошевича, когда приоритетными целями воздушных атак считались ретрансляторные и передающие радио- и телестанции, линии электропередач и т.д. При этом для поражения таких целей использовались и новые образцы нелетального оружия (например, «графитовые бомбы»).

В тех случаях, когда в основе информационной инфраструктуры противника лежит спутниковая связь, нарушение ее работы может осуществляться не только уничтожением самих спутников (если они принадлежат противнику), но и подавлением путем постановки фоновых помех, а также и искажением поступающей по ее каналам информации (что может особенно эффективно осуществляться при использовании противником принадлежащей какой-либо другой стране орбитальной группировки).

Результативность информационных атак на коммуникационные системы противника в значительной мере зависит от масштабов использования в них современных информационных технологий. Причем зависимость эта носит двоякий характер. С одной стороны, широкое использование новейших информационных технологий позволяет создать избыточные резервные каналы связи, подавить которые будет значительно сложнее, чем редуцированную систему, причем одновременно такие каналы могут служить своего рода маскировкой действительно значимых линий связи, обслуживающих командные центры. Использование подобной системы коммуникаций Югославией привело к тому, что представления НАТО о потерях и разрушениях югославских линий связи в ходе воздушных бомбардировок оказались сильно завышенными, в то время как в действительности югославская система управления сохранила свою эффективность. С другой же стороны, отсутствие разветвленной избыточной системы коммуникаций естественным образом уменьшает ее

уязвимость, хотя при этом, безусловно, резко снижается эффективность самих систем контроля и управления.

Избыточность коммуникационных систем должна тщательно продумываться и планироваться, а не являться следствием их хаотического роста. Например, дублирование информационного трафика дает определенную гарантию сохранности поступающей критической информации, в то время как дублирование информационных потоков в редуцированных сетях, особенно при их хаотическом построении, способно вызвать перегрузку вычислительных мощностей системы и привести к прекращению обработки информации. Напрашивается вывод, что живучесть коммуникационных систем в значительно большей степени зависит от их организационного построения, чем от использования новейших информационных технологий.

Несмотря на то, что информационные операции по борьбе с системами контроля и управления стали весьма существенным аспектом современных представлений о ведении войны, они не подменяют собой традиционные способы ведения боевых действий. Особая ценность информационных операций против систем управления состоит в том, что они могут оказаться особенно эффективными на ранних стадиях развития конфликта и, кроме того, создают предпосылки для достижения бескровной победы над противником. Однако эти преимущества могут быть в значительной степени нивелированы противником путем децентрализации командных систем, а также посредством ведения им так называемой «сетевой войны», принципы которой будут рассмотрены ниже.

Информационно-разведывательные операции («цифровое поле боя») Концепция ведения информационно-разведывательных операций в определенном смысле является развитием концепции оперативной разведки, хотя между ними наблюдаются и существенные различия, связанные с тем, что получаемые в ходе информационно-разведывательных операций сведения (например, данные целеуказания или сведения о нанесенном ущербе) поступают непосредственно участникам операции, вплоть до исполнительного уровня (реализация концепции «цифрового поля боя»), в то время как обычно данные военной разведки направляются в командные центры, где они суммируются, обрабатываются и затем в качестве приказов и вводных доводится до подчиненных. По сути дела, речь идет об адаптации оперативной разведки к децентрализованной системе боевого управления и ведения

боевых действий, требующей внесения значительных корректив в архитектуру и идеологию сбора, обработки и распределения разведывательной информации.

Новые децентрализованные автоматические и автоматизированные системы, призванные решать конкретные задачи в ходе информационно-разведывательных операций, сами по себе являются потенциальными объектами рассмотренной выше борьбы с системами управления. В этой связи представляется целесообразным рассматривать два аспекта таких операций: первый, условно называемый «наступательным», обеспечивает сбор разведывательной информации о противнике, а второй, «оборонительный» или «защитный» - связан с защитой собственной информации и противодействием информационно-разведывательным операциям противника.

«Наступательные» информационно-разведывательные операции
Быстрое развитие информационных технологий, возрастание их возможностей при одновременном снижении их относительной стоимости, особенно в области систем передачи и распределения информации, диктует все более острую необходимость создания новой архитектуры систем, предназначенных для сбора и обработки информации, в том числе разведывательной, особенно в военной сфере. Такая архитектура должна обеспечить объединение сенсорных систем, распределителей информации и систем оружия, причем подразумевается, что каждый из элементов будет способен действовать автономно, располагая доступом к обобщенным информационным ресурсам.

Принцип проведения информационно-разведывательных операций и их основное преимущество перед традиционной разведкой состоит в том, что они обеспечивают поступление информации в реальном или близком к реальному масштабе времени, используя адаптируемые алгоритмы доведения неизбыточной информации до непосредственных потребителей и лиц, принимающих решения.

Теория проведения наступательных информационно-разведывательных операций легла в основу концепции «цифрового поля боя», согласно которой получение оперативной информации из района боевых действий обеспечивается комплексным применением систем сенсоров и датчиков с различными уровнями детализации получаемой информации. Всего принято выделять четыре таких уровня:

1. Системы дальнего обнаружения, представленные, в первую очередь, космическими системами слежения и, в определенной мере, сейсмодатчиками и акустическими системами;
2. Системы оперативно-тактического уровня. В качестве таковых могут использоваться: беспилотный летательный аппарат с радиоэлектронным, тепловизионным и другим оборудованием, в том числе обеспечивающим возможность ведения РЭБ; гидроакустические (сонарные) буи, предназначенные для отслеживания ситуации на морских и океанских театрах военных действий, а также определенные типы стационарных наземных радаров. Отработка операций с задействованием систем оперативно-тактического уровня активно проводилась во время Югославского конфликта;
3. Системы тактического уровня, включающие оптические, гравиметрические, биохимические, акустические и прочие сенсоры и датчики;
4. Средства навигации и управления оружием и боевыми платформами.

Создание многоуровневой системы средств «наступательного» сбора данных позволяет получать максимально полную картину ситуации в районе боевых действий и облегчает распределение информации между пользователями. Вместе с тем, для общей интеграции компонентов такой системы требуется разработка особых алгоритмов координации их работы, что представляет собой достаточно сложную задачу. Это обстоятельство обусловливает интенсификацию прикладных разработок в области искусственного интеллекта и систем поддержки процесса принятия решений.

«Оборонительные» информационно-разведывательные операции

Если целью «наступательных» информационно-разведывательных операций является оперативный сбор, обработка и доведение до конечного пользователя максимально полной информации о противнике, то главная цель «оборонительных» операций, соответственно, состоит в недопущении получения противником аналогичной информации о собственных вооруженных силах или же в ее искажении на любом из уровней системы сбора разведданных противника, в том числе при передаче, прохождении, и обработке информации.

Использование таких «оборонительных» методов югославской стороной во время конфликта весной-летом 1999 г. в целом обеспечило ей сохранение управляемости войсковыми подразделениями и минимизировало потери, что впоследствии было подтверждено комиссиями НАТО.

Другим аспектом «оборонительных» информационно-разведывательных операций является защита собственных средств получения информации от средств поражения и мер противодействия противника. Одним из наиболее эффективных способов при этом является упрощение и, соответственно, удешевление систем до такого уровня, когда попытки их физического уничтожения становятся неоправданно дорогими. Если, например, дорогостоящие и малочисленные самолеты дальнего радиолокационного обнаружения достаточно уязвимы и представляют собой достаточно очевидную цель, то применение противником зенитных ракет против более дешевых и многочисленных беспилотных летающих аппаратов становится экономически не оправданным.

Однако следует иметь в виду, что системы сбора и передачи информации могут подвергаться атаке и другими способами, например хакерскими приемами или подавляться системами радиоэлектронного подавления, которые являются самостоятельными направлениями ведения информационной войны.

Методы «защиты», предусматривающие искажение информации, могут оказаться наиболее эффективными в том случае, если соответствующие данные получаются из распределенных систем информации, требующих сравнения и дополнения данных различных источников. Например, при поступлении противоречивой информации по каналам спутниковой сети JSTARS и через разведывательные беспилотные летающие аппараты процесс принятия решений при проведении информационно-разведывательных операций может быть в значительной мере затруднен или даже парализован. Немаловажно также и то, что такие искажения имеют тенденцию к возрастанию по мере прохождения и обработки информации от уровня к уровню, в связи с чем все большую актуальность в настоящее время приобретают работы по созданию систем сравнения и оценки входящей информации в условиях неопределенности.

Электронная борьба

Прежде всего следует отметить, что первые два рассмотренные выше направления информационного противоборства, по сути дела, представляют собой либо борьбу с информационными системами, либо борьбу при помощи информационных систем. В отличие от них целью электронной борьбы как прикладного метода ведения информационного противоборства является снижение информационных возможностей противника, в соответствии с чем она подразделяется на радиоэлектронную борьбу (создание условий, в которых передача или

прием информации противником становится невозможным, в частности из-за постановки активных и пассивных помех), криптографическую борьбу (искажение и ликвидация собственно информации) и борьбу с коммуникационными системами противника.

Радиоэлектронная борьба

Радиоэлектронная борьба как комплекс мероприятий оперативного (боевого) обеспечения, проводимых в целях выявления и последующего подавления радиоэлектронных средств и систем противника (прежде всего приемо-передающих средств), известна уже в течение довольно длительного времени. В настоящее время многие военные эксперты называют ее в числе главных направлений ведения информационной войны в предвоенный и военный периоды.

Средства и методы ведения РЭБ постоянно совершенствуются, в частности предусматривается не только постановка помех, затрудняющих или не допускающих передачу информации, но и использование параметров излучающей аппаратуры противника для наведения на них средств физического поражения, таких как американские противорадиолокационные ракеты HARM. Поскольку при таком наведении на цель используются не пассивные параметры объекта поражения (эффективная поверхность рассеивания, тепловое излучение, визуальный образ), а активные, сама возможность применения противорадиолокационного оружия может затруднить или даже привести к отказу от использования приемо-передающих средств.

Подробно примеры и методы применения средств РЭБ рассмотрены в предыдущей главе.

Борьба с коммуникационными системами

Борьба с коммуникационными системами (линиями связи) противника является значительно более сложной задачей, чем ведение РЭБ. Это определяется прежде всего тем, что приемо-передающие средства уже в силу своей функциональной предназначенности являются достаточно легко обнаружимыми источниками излучения, в то время как излучение линий и каналов связи по возможности снижается до минимально достижимого уровня. В частности, изоляция и экранирование таких линий связи, а также использование волоконной оптики и лазерной техники позволяет в значительной мере избежать не только потерь и искажения информации в силу естественных причин (различного рода электромагнитных наводок, в том числе от постороннего оборудования),

но и перехвата противником данных, передаваемых по этим линиям. Тем не менее, в ряде случаев каналы обмена информацией остаются потенциально уязвимыми, особенно для беспроводной передачи информации с объектов (например, спутников или беспилотных летательных аппаратов), местоположение которых может быть с достаточной точностью определено и зафиксировано. В этом случае такие каналы коммуникаций невозможно полностью изолировать или экранировать, и достаточно эффективным способом борьбы с ними становится постановка хаотических помех, чьей задачей становится не глушение (подавление) приемо-передающих средств, а своего рода заполнение фоновыми или заградительными шумами той среды, в которой осуществляется передача информации. Возможен также и перехват передаваемой информации, даже в случае использования узконаправленных систем связи, однако решение этой задачи осуществляется уже в сфере криптографической борьбы.

Криптографическая борьба

Криптографическая борьба, как средство ведения информационного противоборства, заключается в сокрытии (зашифровке) собственных данных и получении доступа к данным, скрываемым противником. При этом основной принцип защиты информации заключается в том, что расшифровка (которая принципиально всегда возможна) защищенной современными методами криптографии информации является трудоемким и сложным процессом, требующим мощнейшей вычислительной техники и занимающим, как правило, весьма значительное время, в течение которого информация может устареть. Совместное использование различных методов криптозащиты, например комбинированное применение «длинных» ключей и многократного перешифрования данных, делает быструю расшифровку данных крайне маловероятной. Поэтому одной из главных задач, стоящих перед подразделениями криптографической борьбы при расшифровке информации противника, становится предварительное определение ее ценности и того времени, на протяжении которого дешифруемая информация не потеряет своей значимости.

Аналогичная задача должна решаться также и при шифровании собственных данных, поскольку неоправданное применение усложненных методов криптозащиты может повлечь за собой резкое увеличение объема передаваемой информации, снижение скорости ее передачи/приема и общую перегрузку каналов связи. Таким образом, необходимую степень криптозащиты следует определять в зависимости

от ценности информации. В некоторых случаях более целесообразным может явиться даже отказ от криптозащиты и передача вообще незашифрованной информации, которая, таким образом, будет маскироваться под естественный «информационный шум» и, скорее всего, не привлечет излишнего внимания противника.

Психологическая борьба

В тех случаях, когда использование методов информационного противоборства направлено не против информационных систем противника, а непосредственно против человеческого разума и психики, речь идет о психологической борьбе. В самом общем виде психологическую борьбу можно определить как манипулирование общественным сознанием, общественным мнением на различных социальных уровнях. Подробно методы и средства психологического воздействия рассмотрены в предыдущих главах. Здесь же мы остановимся на использовании этих средств в рамках информационного противоборства.

На Западе принято выделять следующие основные категории информационно-психологических операций, проводимых в рамках психологической борьбы:

- операции, направленные против структур государственного управления;
- операции, направленные против структур военного командования;
- операции по деморализации личного состава вооруженных сил.

Информационно-психологические операции, направленные против структур государственного управления

Главными объектами информационно-психологического воздействия в данном случае являются общество в целом и основные структуры государственного управления. При этом наиболее восприимчивым к такого рода воздействию является все же общественное мнение. Государственные структуры, в силу присущей им консервативности (в результате чего их действия подчинены вполне традиционной схеме выбора наименьшего из двух зол), относительно менее восприимчивы к стандартным методам манипулирования общественным сознанием.

Для проведения информационно-психологических операций, целью которых является дестабилизация внутреннего положения в стране противника, в качестве наиболее эффективного канала выступают СМИ. При этом могут применяться различные способы оказания воздействия

через СМИ, в том числе и связанные с воздействием на инфрастуктуру самих СМИ. Можно выделить несколько в общем хронологически следующих друг за другом этапов оказания такого воздействия, которые ниже располагаются в порядке убывания их эффективности:

- оказание воздействия через национальные СМИ противника;
- в случае, если это невозможно, а также в целях достижения большего эффекта — формирование альтернативных каналов информационно-психологического воздействия (альтернативные СМИ, иновещание и т.п.). Ключевую роль при этом в настоящее время начинает играть глобальная информационная сеть интернет;
- оказание внешнего давление на политическое руководство и общественное мнение государства-противника, создание международного климата, препятствующего реализации планов противника;
- подавление существующих систем национального вещания, например уничтожение ретрансляционных спутников, телевизионных и радиовещательных станций и т.п.

Информационно-психологические операции против командных структур
Дезорганизация командования и управления войсками противника является первостепенной задачей при ведении не только информационной войны, но и обычных боевых действий. Вместе с этим, по мнению аналитиков INSS, прямая пропагандистская борьба против командования едва ли будет иметь успех. Если рассматривать типичную модель государственного строения, то военное руководство любого уровня является инструментом, выполняющим волю политического руководства государства и, следовательно, не играет решающей роли в процессах выработки и принятия политических решений. Поэтому в качестве одного из основных средств, используемых в ходе информационно-психологических операций против командных структур, прежде всего является дезинформация.

Некоторые из теоретических положений западных ученых, касающихся психологических операций в этой области, выглядят непривычно, однако предпринимаемые на их основе мероприятия могут оказаться достаточно эффективными и действенными. Например, общепринято, что решения принимаются военным командованием на основе анализа сложных и, как правило, слабо поддающихся прогнозированию событий. Следовательно, если, учитывая такое положение, не ограничивать возможности получения информации противником, а напротив, предоставлять ему избыточную и противоречивую информацию о происходящих событиях,

то в условиях ограниченного времени принятие адекватных решений и сам процесс командования и боевого управления может быть в значительной степени нарушен.

Не меньшую роль в дезорганизации деятельности командных структур может играть устрашение. В частности, эффективным считается формирование у противника устойчивого мнения о превосходстве другой стороны и о бессмысленности сопротивления. Однако такая информация может быть и объективной. Вообще говоря, ключевым моментом в дезорганизации противника является стирание грани между возможным, реально существующим и невозможным. Для достижения этой цели была предложена «стратегия навязанной стоимости». Ее автор, полковник ВВС США Д. Уорден[2] полагает, что если противнику удастся навязать такой образ действий, который впоследствии окажется слишком затратным для него, он в конце концов откажется от продолжения борьбы. Реализация этой стратегии предполагает проведение следующих мероприятий:

- оценка ценностей противника, его сильных и слабых сторон;
- определение на основе полученной системы оценок «болевого порога» противника;
- осуществление информационных операций, направленных на достижение и превышение этого порога, с целью вызвать частичный паралич и создать угрозу полного паралича в деятельности командных структур.

Высказывается также мнение, что в ряде случаев действия в кризисной ситуации можно будет ограничить только демонстрацией возможностей, т.е. конфликт будет разрешен уже на фазе психологической обработки управляющего звена противника.

С рассмотренной стратегией в значительной мере коррелирует так называемая стратегия паралича, цель которой — сделать невозможным дальнейшее продолжение сопротивления со стороны противника. При этом формулируется следующая иерархия основных целей воздействия в ходе соответствующих информационных операций:

- политическое и военное руководство страны;
- базовое производство (промышленность, энергетика);
- инфраструктура (транспорт, коммуникации);
- население;
- воинские подразделения.

[2] The Changing Role of Information in Warfare. RAND, 1999.

Что касается степени воздействия на систему в целом, то она будет определяться выбором конкретной цели или их совокупности.

Деморализация вооруженных сил
Психологические операции против личного состава вооруженных сил противника базируются на использовании двух основных присущих человеку чувств: страха смерти и взаимной неприязни, а также на отсутствии непосредственной связи между передовой и тылом. Для решения задачи деморализации личного состава предлагается задействовать как традиционные (листовки, радиовещание и т.п.), так и новые способы пропаганды.

По некоторым оценкам, значительный эффект может быть получен при предоставлении правдоподобной, но провоцирующей страх или чувство неудовлетворенности информации непосредственно каждому участнику боевых действий со стороны противника. Например, для этого во время Югославской войны на предполагаемые позиции югославской армии сбрасывались приемники, настроенные на фиксированную волну специальной радиостанции НАТО. Однако, насколько можно об этом судить в настоящее время, большого успеха такая методика не принесла.

Другим перспективным методом проведения информационно-психологических операций в условиях конфликтов низкой интенсивности (когда «передовая» и «тыл» располагают весьма ограниченной информацией друг о друге) считается предоставление им раздельной и дозированной информации. При этом предполагается задействовать и национальные информационные каналы противника.

Хакерская борьба
Понятие хакерской борьбы сводится главным образом к осуществлению «атак» на различные компоненты компьютерных сетей и хранящиеся в них информационные ресурсы. Основной особенностью хакерских «атак» является то, что они носят не аппаратный, а программный характер. Это означает, что используемая хакером программа проникновения способна обнаруживать уязвимое место в структуре защиты компьютерной системы противника и проникать через нее, что в результате дает возможность управлять работоспособностью системы или манипулировать (стирать, изменять) содержащуюся в ней информацию. Некоторые западные аналитики, например, В. Швартау и Р. Хаени[3], склонны даже считать, что

[3] Winn Shwartau, Draper John. Cybershock. Thunder's mouth pr., National books, 2000; Haeny Rato. Information warfare. An introduction. Washington, The George Washington University Cyberspace Institute, 1997.

информационное противодействие в целом может быть сведено исключительно к хакерской борьбе.

Конкретные приемы хакерской борьбы носят самый разнообразный характер. Их целью может являться как полное выведение из строя компьютерных систем, так и инициирование различных периодических или приуроченных к конкретному моменту времени сбоев в работе, выборочное искажение содержащихся в системе данных, получение доступа к системной информации (пароли, адреса), несанкционированный мониторинг работы системы, искажения трафика сообщений. Наиболее популярными из используемых в настоящее время средств являются так называемые компьютерные вирусы, «черви», «троянские кони», логические бомбы, «дыры» в системе, прошивка постоянного запоминающего устройства. Перечисленные средства, наряду с постоянно появляющимися новыми программными средствами хакерских атак, могут, по мнению Р. Хаени[4], рассматриваться как существующие и потенциальные образцы информационного оружия.

Компьютерные вирусы

Компьютерный вирус по своей сути является фрагментом программного кода, способным самокопироваться («размножаться») путем записи своей копии в коды других программ компьютерной системы, подвергающейся компьютерному проникновению. Такой вирус является средством нарушения работоспособности компонентов программного обеспечения или локальной системы.

Компьютерный вирус активируется при запуске программы, в которую он внедрен, после чего он может либо скопировать себя в другую программу, либо выполнить действия по искажению данных или нарушению работоспособности системы. Считается, что компьютерные вирусы в ряде случаев могут целенаправленно использоваться при ведении информационной войны в целях нарушения работоспособности компьютерных систем противника. Так, в прессе появляются сообщения, что специалисты Тайваня разработали несколько тысяч новых, своего рода «боевых» компьютерных вирусов для использования против компьютерных систем КНР на случай возникновения кризисной ситуации в отношениях между ними.

Существенным недостатком компьютерных вирусов с точки зрения ведения организованной информационной войны является их почти полная

[4] Ibid.

автономность (за исключением необходимости запуска программы-«хозяина»), в результате чего практически не существует возможности контролировать и корректировать их работу в системе противника.

«Черви»

В отличие от компьютерных вирусов, «червь» представляет собой самостоятельный программный пакет, предназначенный для самораспространения путем копирования своего пакета с одного компьютера на другой, как правило, через сеть, в том числе и интернет. Другое важное отличие «червя» от вируса состоит в том, что он не модифицирует программы компьютерной системы и не повреждает данные на локальном компьютере, а позволяет в соответствии со своим предназначением нарушать работоспособность сети или получать доступ к информационным ресурсам сети, подвергшейся атаке. В ряде случаев, когда работоспособность тех или иных организаций или структур напрямую зависит от стабильности работы используемой корпоративной компьютерной сети, например в банковской сфере, использование «червей» как вида информационного оружия может оказаться весьма эффективным.

«Троянские кони»

«Троянский конь» представляет собой фрагмент компьютерного кода, скрытый внутри инфицированной программы, и является широко используемым механизмом маскировки проникновения вирусов или «червей» в систему.

«Троянские кони» могут маскироваться, в частности под служебные программы, поставляемые с коммерческими и иными программными комплексами обеспечения безопасности компьютерных систем. Примером может служить комплекс «Сатан» (административные средства безопасности для сетевого анализа), предназначенный для поиска программных «дыр» в Unix-системах и бесплатно распространяемый по сети интернет. Потенциальный злоумышленник может модифицировать часть программного обеспечения комплекса, а затем предоставить модифицированную версию к дальнейшему распространению. Грамотно написанная программа-«троянец» практически не оставляет следов своего присутствия, а поскольку она сама по себе не вмешивается в работу системы, то ее очень трудно обнаружить.

Логические бомбы

Логическая бомба является разновидностью «троянского коня» и используется для инициирования вирусной или иного рода программной

атаки на компьютерную систему. Наиболее известным и распространенным является срабатывание логической бомбы на заранее заданный контекст (ключевое слово).

Логическая бомба может быть самостоятельной программой или фрагментом кода, распространяемым программистами или производителем некоторого программного продукта (пакета программ). В настоящее время, когда практически во всем мире используются главным образом американские программные продукты (например, MS Windows или Unix), ставшие своего рода стандартом, использование логических бомб становится вполне вероятным, причем инициаторами этого могут выступать не только производители программного обеспечения, но и правительство страны-производителя.

«Дыры» в системе, черные ходы

«Черными ходами» называются специальные программные механизмы, действующие в обход систем безопасности и встраиваемые в систему производителем программного обеспечения с целью получения доступа производителя (или лица, чьи интересы он обеспечивает) к информационным ресурсам и настройкам системы. Этот метод считается наиболее привлекательным для проведения информационно-разведывательных операций. Напомним лишь, что осенью 1999 г. в США разразился достаточно громкий скандал, связанный с тем, что одному из программистов удалось выявить такие «черные дыры» в программных продуктах фирмы «Майкрософт» — разработчика самой популярной и широко используемой на настоящий момент времени системы MS Windows.

«Прошивка» постоянного запоминающего устройства

Точно так же, как в программное обеспечение могут быть заложены компоненты, выполняющие непредусмотренные функции, производители аппаратного обеспечения, прежде всего, устройств с постоянными запоминающими устройствами (например, BIOS) могут внедрять логические бомбы или устанавливать «черные ходы» в компьютерных системах. Изменения в программное обеспечение различных ПЗУ могут быть внесены и другими лицами, что, например, уже делалось при перепрограммировании модемов. С широким использованием флэш-BIOS процедура внесения таких изменений значительно упростилась и не требует сложного оборудования.

Следует отметить, что рассмотренный выше арсенал хакерских средств, который может применяться при ведении информационной войны,

широко используется также одиночными лицами-злоумышленниками («компьютерными пиратами»), что существенно затрудняет задачу выявление источника агрессии и целей, преследуемых в ходе той или иной атаки, а также выбор адекватных форм реагирования.

Кибернетическая и сетевая борьба

Концепции «кибернетической» и «сетевой борьбы», несмотря на вполне «техническое» русское звучание, в наименьшей степени связаны с собственно информационными технологиями и охватывают полный комплекс проблем и аспектов информационного противоборства (организационные, доктринальные, стратегические, тактические и технические стороны ведения наступательных и оборонительных информационных операций).

Так, концепция кибернетической борьбы, относящаяся к информационно-ориентированным военным операциям, в настоящее время становится все более актуальной именно в военной сфере, особенно когда речь идет о конфликтах высокой интенсивности. Кибернетическая борьба нашла свое отражение также в более широкой концепции «революции в военном деле» — использования новых технологий и, что особенно важно, осуществления организационных и управленческих изменений в военной области. Эта концепция является самостоятельным объектом изучения и в настоящей работе не рассматривается.

В то же время роль сетевой борьбы возрастает в конфликтах низкой интенсивности и при проведении так называемых «операций, отличных от войны», а также в конфликтах, террористических действиях и иных преступлениях, носящих невоенный характер. При этом понятие сетевой борьбы относится скорее к организационной форме противоборства, использующей информационные возможности, чем собственно к борьбе с информационными инфраструктурами противника. Более того, концепция сетевой борьбы подразумевает использование информационных инфраструктур противника в своих целях. В этом отношении данный вид информационного противоборства имеет много общего с ведением террористической борьбы, в которой главными действующими лицами выступают небольшие взаимосвязанные и координирующие свои действия группы, не имеющие единого командования. В таком случае можно говорить, что их структура строится не на иерархическом, а на сетевом принципе, и именно в этом заключается главное отличие информационно-ориентированной сетевой борьбы от социальных конфликтов и преступлений, где в качестве действующих лиц выступают разрозненные

иерархические организации, имеющие жесткие и изолированные идеологии, доктрины и стратегии борьбы.

В качестве примеров, иллюстрирующих отмеченные различия иерархических и сетевых структур, можно привести особенности стратегий ряда экстремистских и террористических организаций. Так, «Хамаз», по утверждению израильских источников, в значительно большей степени использует возможности сетевой борьбы, чем Организация освобождения Палестины. То же самое можно сказать в отношении Американских христианских патриотов и Ку-Клукс-Клана.

Характерная особенность сетевой борьбы состоит в том, что подавляющее большинство, если не все действующие лица, использующие методы такой борьбы, являются негосударственными организациями. Среди них могут быть: транснациональные террористические группы, нелегальные торговцы оружием, транснациональные преступные синдикаты, наркомафия, фундаменталисты, этнонационалистические движения, информационные пираты, контрабандисты и т.п. Таким образом, на государственном уровне сетевая борьба сводится прежде всего к противодействию такого рода организациям, использующим сетевые организационные методы, т.е. к антитеррористической борьбе.

Можно выделить три основные проблемы, возникающие при ведении государственной контрсетевой борьбы:

1. Иерархические государственные системы, как правило, оказываются малоэффективными при борьбе с сетевыми структурами. Это связано прежде всего с тем, что время, необходимое для принятия решений и адекватного реагирования на происходящие изменения в обстановке, в иерархических системах значительно превышает аналогичные показатели сетевых структур.
2. Эффективная антитеррористическая борьба требует формирования антитеррористических подразделений, строящихся на сетевой основе и, следовательно, наделенных расширенными полномочиями в вопросах принятия решений. Данное требование не подразумевает зеркального копирования структуры и методов террористических организаций, с которыми ведется борьба. Значительную роль в решении этой проблемы могут играть технические нововведения, выработка новых механизмов межведомственного координирования, а также развитие межгосударственной кооперации, включая, в том числе, унификацию национальных законодательных систем.

3. Получение преимущества в сетевой борьбе в значительной степени определяется тем, насколько эффективно используются возможности, предоставляемые сетевой организацией и информационными сетями (интернет).

В частности, с решением всех этих проблем пришлось столкнуться американским специалистам при создании специального контртеррористического центра, функционирующего при ЦРУ. С одной стороны, в работе этого центра используются функциональные принципы сетевой организации, а с другой — осуществляется активное взаимодействие с традиционными военными и государственными иерархическими институтами.

Экономическая информационная война

В последние годы возрастает озабоченность возможностью использования методов и средств информационной войны в экономической сфере, в связи с чем западные специалисты выделяют две основные формы экономического информационного противоборства: информационную блокаду и информационный империализм. Следует отметить, что речь ниже будет идти прежде всего о стратегии, а не о конкретных технологических решениях, которые могут изменяться с течением времени.

В настоящее время информационные сети обеспечивают доступность информации пользователю практически в любом месте планеты. Изменились также и темпы устаревания информации: если еще в начале XX века скорость информационных потоков измерялась скоростью передвижения курьеров, в середине века — скоростью почтовых перевозок, то в настоящее время она ограничивается лишь пропускной способностью коммуникационных линий, т.е. информация передается практически в реальном масштабе времени. Это обстоятельство является чрезвычайно важным, особенно для международных экономических процессов, и означает, что государственные границы и большие расстояния уже не играют столь значительной роли, как в прошлом, и на первый план начинают выступать транснациональные структуры и организации.

Информационная блокада

По мнению аналитиков, современные развитые общества примерно в одинаковой мере зависят от стабильности информационных потоков и от материальных поставок. При этом нормальное функционирование ряда

сфер экономики и финансов целиком зависит от возможности и своевременности получения доступа к информационным ресурсам. Более того, процессы глобализации мировой экономики и развития неденежной экономики превращают зависимость финансового сектора от информационных и обслуживающих технологий практически в абсолютную.

В таких условиях экономическая информационная блокада становится крайне гибким и эффективным методом воздействия на потенциального противника. В отличие от введения эмбарго на тот или иной вид товаров или других экономических санкций, информационная блокада может носить скрытый характер, а соответствующие информационные операции могут быть завуалированы под случайные сбои информационных систем или случайные хакерские проникновения компьютерных хулиганов. При этом, естественно, не снимается возможность и открытого государственного давления в этой области. Например, в ходе операции «Буря в пустыне» и во время войны в Югославии были заморожены счета этих стран, размещенные в банках США и Европы.

Вместе с тем, информационная блокада все же является одним из крайних средств в перечне возможных средств воздействия на потенциального противника, и ее эффективность во многом определяется уровнем контроля над информационными ресурсами в глобальном масштабе. В связи с этим постоянно нарастает актуальность второго направления экономического информационного противоборства — информационного империализма.

Информационный империализм

Как уже отмечалось, глобализация мировых экономических процессов обеспечивается постоянно ускоряющимся развитием современных информационных технологий, поэтому не удивительно, что наиболее приспособленными к эффективной экономической деятельности в новых условиях оказались технологически развитые государства, среди которых бесспорным лидером выступают США. Не является секретом, что разработка основных компонентов компьютерной техники и общего программного обеспечения сосредоточена, прежде всего, в этой стране. Например, тенденции развития средств телекоммуникаций во многом диктуются американским концерном AT&T, а важнейшее место на рынке предоставления провайдерских услуг (обеспечение доступа в интернет) принадлежит компании «Америка Онлайн», которая, в частности, контролирует и каналы подключения России к этой сети.

Большинство аналитиков отмечает, что уже на современном этапе сама структура информационных коммуникаций начинает существенно изменяться. Если в начале своего функционирования интернет рассматривался преимущественно в качестве некоторого множества информационных ресурсов, и основной его задачей считалось оказание помощи в поиске нужной информации и организации доступа к ней, то на нынешнем («коммуникационном») этапе развития главной задачей интернета считается оказание помощи при поиске требуемых партнеров и организации между ними нужного вида коммуникаций с необходимой интенсивностью (увеличение «виртуальной» деловой активности).

Отчетливо прослеживаются две главные тенденции в развитии информационных коммуникационных услуг, в соответствии с которыми:

- человек в ближайшем будущем будет получать только ту информацию, которая его интересует, и прямо из того места, где эта информация рождается;
- любой человек или компания может с небольшими затратами открыть в интернете свой собственный канал вещания, что приведет к появлению миллионов независимых информационных каналов.

Можно предположить, что такие нововведения существенно изменят ту часть бизнеса, которая занимается выпуском различных периодических изданий и другой информационной продукции. В частности, уже сегодня практически все известные издания мира имеют собственные электронные версии в интернете. Одновременно с этим повышается актуальность проблемы прямого проникновения иностранных кампаний на внутренний рынок.

Наибольшее влияние «информационной революции» испытала на себе международная финансово-кредитная сфера. В результате развития средств автоматизации финансовых операций была создана международная телекоммуникационная банковская система «Свифт», объединившая свыше 2000 банков в 60 странах мира. Надежность данной системы достигается ограничением доступа к сети — к работе в ней допущены только сертифицированные банки, а любая попытка взлома этой системы влечет за собой немедленное удаление из нее нарушителя.

В систему «Свифт» уже вошли все крупные и значительная часть средних российских банков. Это обстоятельство, безусловно, говорит об интеграции российских финансовых институтов в международную финансовую систему и об имеющейся возможности быстрого получения

и обмена информацией, однако не следует забывать, что одновременно данная система может использоваться для контроля и управления валютно-финансовой ситуацией в мире со стороны ведущих американских банков. О такой возможности говорит автоматическое «замораживание» иракских вкладов после того, как США наложили эмбарго на вклады Ирана во время обострения отношений с этой страной в середине 80-х годов. Тогда в течение нескольких дней руководители многих банков не имели представления о местонахождении иранских вкладов, хранившихся ранее на их счетах.

Процесс «виртуализации» мировой экономики привел к тому, что общий объем капиталов на финансовых рынках на порядок превосходит мировой ВВП. Одновременно развитие технических возможностей средств связи, передачи и накопления информации (телевидение, компьютерные системы и локальные сети, интернет) привело к резкому возрастанию мобильности капиталов, а также к резкому возрастанию чувствительности мировых финансово-экономических и социальных процессов к информационным воздействиям.

Непосредственным следствием информационной революции стало сокращение числа филиалов крупных западных банков и создание вместо них сети банкоматов и электронных систем самообслуживания. Выездные банковские услуги, бывшие ранее прерогативой исключительно крупных высокообеспеченных клиентов, в настоящее время становятся общедоступными, а на смену выездных операционистов и разветвленной структуры филиалов приходят те или иные электронные услуги — магнитные и чиповые карты (смарт-карты), управление счетами по телефону и через интернет. При этом скорость совершения банковских операций многократно увеличивается.

Следствием ускоренного перехода от наличных расчетов к электронным являются, с одной стороны, создание достаточно прочной базы для осуществления государственного контроля и регулирования финансовых потоков, а с другой — повышение уязвимости компьютерных банковских сетей по отношению к различного рода махинациям. Так, по оценке ФБР, ежегодные финансовые потери от действий «хакеров» только в США составляют пять миллиардов долларов. Однако для финансовых институтов привлекательность постоянно расширяющейся всемирной сети остается весьма высокой.

Существует также опасность монополизации сферы электронных финансовых расчетов. Так, Министерство юстиции США с 1996 г.

проводило расследование нарушения антитрестовского законодательства системами кредитных и дебетовых карт «Виза» и «Мастеркард», и осенью 1998 г. выдвинуло против них иск в федеральном суде штата Нью-Йорка. Суть дела состоит в том, что этими платежными системами владеет одна группа крупнейших банков, сосредоточившая тем самым в своих руках 75% американского рынка электронных карт, в то время как на карты «Американ Экспрес» приходится 18,4%, «Дискавер» — 5,6%, «Динерс Клаб» — 1%.

Российские банки не остаются в стороне от внедрения электронных банковских операций. Здесь следует отметить прежде всего совместный проект АО «МГТС» и Гутабанка — систему «Телебанк», позволяющую управлять банковским счетом по телефону, однако данная система не заменяет, а лишь дополняет традиционные банковские услуги. Достаточно высокая плата за пользование этой системой говорит о том, что в ближайшей перспективе она вряд ли сможет стать сколько-нибудь массовой. В настоящее время общее число ее клиентов составляет лишь несколько тысяч человек.

Фактическое отсутствие национальных информационных коммуникаций является одной из наиболее серьезных проблем, с которыми сталкивается Россия в информационной сфере. Существующая информационно-коммуникационная структура России ориентирована на западных производителей и провайдеров. До настоящего времени не создано даже единой национальной сети для обслуживания государственных и коммерческих организаций. До последнего времени создание подобных корпоративных сетей протекало на уровне хаотичного, не координированного их формирования в качестве сегментов сети интернет. Это вызывает закономерные опасения специалистов и аналитиков, поскольку делает отечественные корпоративные сети потенциально «прозрачными» для создателей и пользователей «глобальной паутины» и ставит Россию в определенную зависимость от благосклонности западных государств, прежде всего США.

Информационное противоборство и международный информационный терроризм

В связи с быстрым развитием информационных технологий проблема международного терроризма приобретает в условиях информационного противостояния новое звучание. Это связано, прежде всего, с двумя аспектами: с использованием террористами информационной инфраструктуры для развития так называемых сетевых способов

собственной организации, а также с собственно террористическим воздействием на объекты информационных инфраструктур.

По мнению многих экспертов, террористические организации, независимо от мотивации их действий, постепенно трансформируются от первоначальной иерархической структуры к информационно-ориентированной сетевой организации. Внутри групп личностное влияние лидера все больше уступает место упрощенной децентрализованной системе. Разрозненные группы все чаще сливаются в транснациональные террористические сообщества.

Традиционно принято рассматривать три основные террористические парадигмы: терроризм как средство принудительной дипломатии, терроризм как война и терроризм как предвестник «нового мира». До последнего времени главенствующую роль играла парадигма принудительной дипломатии. Однако изменение организационной структуры террористических групп повлекло за собой изменение стратегии и тактики их действий. В частности, наряду с сохранением принципов воздействия на объекты, разрушение которых может повлечь за собой значительные жертвы у населения и вызвать значительный политический и общественный резонанс, происходит трансформация взглядов на террористическую борьбу как на непосредственное средство достижения цели. Систематическое нарушение работоспособности информационных инфраструктур оказывается даже более эффективным, чем «точечные» террористические воздействия. Более того, переход от изолированных действий к проведению целенаправленных террористических кампаний, зачастую не ограниченных действиями одной группировки и носящих комплексный характер воздействия, многократно усложняет противодействие терроризму.

Борьба с терроризмом может быть осложнена также расширением возможностей для террористических действий. Если до последнего времени терроризм был уделом малочисленных и, по-своему профессиональных групп, то широкое распространение информационных технологий позволяет даже любителям использовать «хакерские» методы, в том числе в террористических целях. Учитывая критическую зависимость многих областей жизнедеятельности от информационных систем, действия такого рода «любителей» становятся не менее опасными, хотя они могут даже не подозревать о возможных последствиях своих действий.

Кроме того, не связанные инертностью развития государственных институтов террористические организации, как правило, значительно быстрее берут на вооружение перспективные информационные технологии, используемые ими как для проведения непосредственных террористических операций, так и для поддержки внутренней организации и координации действий. Многие аналитики даже склонны считать неверными спекулятивные рассуждения о том, что террористы будут предпринимать попытки нарушить работоспособность информационных сетей в целом. Они, по-видимому, будут больше заинтересованы в сохранении работоспособности таких сетей, что позволит им лучше и оперативнее координировать свои действия, а также (о чем свидетельствует опыт работы в сети интернет) маскировать такие действия и пропагандировать свои взгляды. Таким образом, любая открытая информационная инфраструктура потенциально несет в себе опасность использования ее террористическими группами.

И, наконец, следует учитывать возможность того, что государства, проводящие информационные операции, будут маскировать свои действия под террористическую деятельность некоторых известных или неизвестных групп. В этой связи наряду с проблемами поиска стратегии защиты от террористического воздействия все большую остроту приобретают задачи идентификации противника в информационном пространстве и адекватного реагирования на возникающие вызовы.

Для решения этих задач критически важным является определение того, что явилось причиной неисправности работы информационных структур: случайный внутренний сбой или преднамеренная атака. Причем даже незначительные, на первый взгляд, внутренние сбои могут приводить к достаточно серьезным повреждениям, как это, например, произошло 15 января 1990 г., когда сбой в системе американской компании AT&T привел к обрыву на 10 часов международной телефонной связи. Если бы подобная неисправность была идентифицирована как преднамеренная атака, в соответствии с чем была бы применена стратегия сдерживания, последствия могли бы быть гораздо более серьезными. Таким образом, определение факта атаки на информационные инфраструктуры требует выработки соответствующих критериев и создания «системы раннего предупреждения», подобной созданной в годы «холодной войны» системе предупреждения о ракетном нападении. Однако, как уже упоминалось, это представляется затруднительным в силу постоянной и быстрой эволюции характера угроз в информационной сфере.

После обнаружения факта атаки необходимо идентифицировать ее источник, что представляет собой еще более трудную задачу. В случае проведения крупномасштабной длительной атаки задача несколько упрощается, однако при этом масштабы нанесенного ущерба могут поставить под вопрос саму необходимость идентификации источника нападения. В большинстве же случаев источник информационного воздействия может не иметь четкой территориальной привязки. Атака враждебной стороны на информационные инфраструктуры может производиться с территории третьего государства или даже с территории государства, подвергшегося нападению. Еще одна сложность заключается в интернационализации производства компьютерных компонентов, когда, например, при производстве навигационной авиационной системы часть подсистем производится в США, часть — в Юго-Восточной Азии, а программное обеспечение пишется, например, в Индии. В результате, если спустя несколько лет из-за срабатывания логической бомбы происходит катастрофа, то определить, кем именно была «заложена» эта бомба, становится практически невозможным.

Не исключается и вариант, когда в качестве враждебной стороны может выступать не государство, а террористическое сообщество, использующее в своих действиях информационную инфраструктуру дружественной страны. При этом даже в случае точного определения источника атаки оказывается затруднительным принятие адекватных ответных мер.

Меры защиты от информационных террористических атак на объекты информационных инфраструктур могут предприниматься на локальном и национальном уровнях.

Однако практика осуществления мероприятий по обеспечению компьютерной безопасности показывает, что как бы не были хорошо продуманы меры локальной защиты, они не могут гарантировать безопасности при воздействии высококвалифицированных специалистов-хакеров, организованных групп или государств. Защита в этих случаях осложняется постоянным расширением программных и аппаратных средств, и полная защита от всех непредвиденных обстоятельств, особенно от атак низкого уровня, считается в настоящее время невозможной.

Россия в информационном противоборстве

Перед Россией в рамках ведущегося информационного противоборства встают две взаимосвязанные проблемы. С одной стороны, вовлеченность

в мировые процессы информатизации, интегрированность в информационное пространство являются необходимыми условиями для дальнейшего развития всех сфер общественной жизни, приобретения и приумножения авторитета в мировом сообществе. С другой стороны, широкомасштабное распространение информационных технологий, не знающих границ и практически не имеющих барьеров, приводит к возникновению новых угроз безопасности личности, общества и государства в Российской Федерации.

Одной из потенциальных угроз интересам России является тенденция разрешения существующих межгосударственных противоречий путем воздействия на информационную сферу, а часто посредством воздействия на массовое сознание населения другого государства. По сути, это и есть реальная информационная война, скрытая или обличенная в форму информационного противоборства. Несмотря на такой «военный» термин, действия, подпадающие под определение информационной войны, могут вестись и ведутся и в мирное время, особенно интенсивно в периоды различного рода локальных конфликтов, межэтнических и межконфессиональных столкновений.

Вместе с тем по сравнению с большинством стран российское информационное пространство характеризуется большой уязвимостью, одним из факторов которой является низкий уровень развития коммуникаций и огромная протяженность страны. Как следствие, информационный контроль России над ее Севером и Востоком чрезвычайно затруднен, что порождает прямые геополитические последствия в отношениях России с другими государствами, в первую очередь с Китаем, который, как полагают некоторые российские специалисты, использует слабый российский информационный контроль над Дальним Востоком для установления сферы непрямого китайского контроля над регионом[5].

Падение уровня промышленного производства, в том числе информационных технологий в России, повлекло за собой резкое сокращение возможности создания конкурентоспособных отечественных средств информатизации. В результате российские средства вычислительной техники не только не получили места на международном рынке, но и в самой России в преобладающем большинстве используются аппаратно-программные средства и связное оборудование, произведенные за рубежом.

[5] См.: Модестов С.А. Информационное противоборство как фактор геополитической конкуренции. М., Издательский центр научных и учебных программ; Московский общественный научный фонд, 1999, 80 с.

В итоге, для России в настоящее время стала актуальной проблема использования практически исключительно иностранных информационных средств и технологий: телекоммуникационного и иного связного оборудования, компьютерной техники, программного обеспечения[6]. В критическом состоянии находится орбитальная группировка отечественных спутников связи, имеется целый ряд других проблем, обусловленных, в частности, недостатком инвестиций.

О зависимости России от предоставления коммуникационных услуг американской стороной говорит факт отключения ее в начале января 1997 г. от системы «Американ Онлайн», являющейся основным шлюзом выхода российских провайдеров в интернет. В результате не только резко снизились скорости передачи информации и объемы информационных потоков, но и значительно (в десятки раз) увеличились тарифы на почтовые отправления и передачу факсимильных сообщений. К счастью, сложившаяся ситуация была быстро исправлена, однако сама возможность подобного отключения России от мировых информационных и коммуникационных ресурсов по-прежнему существует.

Все это создает условия для закрепления на отечественном рынке иностранных компаний, работающих в этой области. В результате денежные средства, которые могли бы пойти на восстановление российской промышленности, уходят за рубеж, а, кроме того, преобладающее использование средств вычислительной техники и связи, программного обеспечения иностранного производства делает информационную сферу зависимой от развитых государств.

Между тем развитые страны, прежде всего Европы и Азиатско-Тихоокеанского региона, принимают активные меры к защите своего информационного пространства, создают наиболее благоприятные условия для отечественных производителей. Так, по данным СМИ, Министерство иностранных дел и Бундесвер Германии запретили использовать на своих служебных компьютерах программы американской компании «Майкрософт».

Следующим фактором, негативно сказывающимся на состоянии защищенности интересов России в информационной сфере, является неоднородность информационного пространства, возникновение в нем

[6] Надо признать, что эта проблема далеко не только российская: большинство, в том числе развитых, стран в той или иной степени стоят перед ее решением.

культурно-языковых подпространств, не вписывающихся в интеграционные тенденции. Это обусловлено как стремлением к максимальной власти региональных элит, так и действиями экстремистских, зачастую преступных организаций, прикрывающихся различными национальными и религиозными идеями.

Таким образом, Россия оказывается перед угрозой широкомасштабных акций информационного противоборства, направленных на ее информационные ресурсы, систему принятия решений органами государственной власти, а также на массовое сознание населения. В этой связи в последнее время появляются высказывания о необходимости изолировать российское общество от мирового информационного пространства. Однако представляется, что куда большую угрозу для будущего России представляет именно отрезанность от мировых информационных ресурсов, от всеобщего обмена информацией и знаниями, являющегося одним из основных достижений цивилизации на современном этапе развития. Только ускоренное развитие современных информационных технологий и интеграция в мировое информационное пространство может обеспечить как экономический рост в стране, так и приобретение авторитета на международной арене.

Поэтому наиболее рациональным путем защиты от угроз в информационной сфере будет не пассивное, а активное им противодействие, заключающееся в выработке и реализации мер по прогнозированию, выявлению, предупреждению и пресечению угроз на ранней стадии, до их непосредственного воздействия.

При этом следует иметь в виду, что информационное противоборство, как уже отмечалось, подразумевает под собой как воздействие на информационную сферу противника, так и принятие ряда мер по выявлению и защите своих элементов информационной инфраструктуры от деструктивного управляющего воздействия. Оно может быть как информационно-психологическим, объектом которого является общество, социальные группы людей или отдельные личности, так и информационно-техническим, нацеленным на различного рода технические системы[7].

Одним из методов информационного противоборства является анализ информации, циркулирующей в информационном пространстве. Целями

[7] См.: Модестов С.А. Цит.соч.

этого могут быть сбор разведывательной информации, выявление признаков подготовки и осуществления деструктивного и управляющего информационного воздействия на национальные информационные ресурсы, противодействие террористическим и иным преступным посягательствам на элементы отечественного информационного пространства.

Широкомасштабную систему контроля за сообщениями, циркулирующими в системах кабельной и радиосвязи, включая спутниковые каналы, по телефонным и компьютерным сетям, подводным волоконно-оптическим линиям связи, разработало Агентство национальной безопасности Соединенных Штатов Америки. Эта система получила название «Эшелон». В ней участвуют не только США, но и Великобритания, Канада, Австралия и Новая Зеландия. С использованием системы «Эшелон» разведслужбы США могут получать информацию, передаваемую по правительственным, дипломатическим, коммерческим и военным линиям связи, а, кроме того, ежедневно отслеживать до одного-двух миллиардов телефонных переговоров и интернет-сообщений, осуществляя среди них поиск нужной информации.

США и другие страны, участвующие в этой системе, категорически отрицают ее использование в целях, не связанных с борьбой с терроризмом и оборотом наркотиков, — для получения экономической, политической и иной информации. Однако имеется информация, свидетельствующая об обратном. Так, технический консультант Европарламента А. Помпиду утверждает, что именно благодаря «Эшелону» французская фирма «Томсон-СиЭсЭф» потеряла крупный контракт с Бразилией на создание радарных комплексов из-за того, что американской стороне стали известны детали готовящейся сделки. В результате контракт получила американская фирма «Рэйтеон».

Вместе с тем ряд европейских стран планирует создание совместно с США новой глобальной системы контроля за информацией. Таким образом, складывается парадоксальная ситуация: европейские страны выступают против использования системы «Эшелон» только, если они сами в ней не участвуют. Это говорит о том, насколько большое значение страны Запада придают контролю за информационным пространством, а также показывает, что вектор противоборства смещается именно в информационную сферу.

Кроме «Эшелона» американские ведомства активно внедряют в практику контроль за электронной почтой с использованием системы «Хищник».

Принцип ее действия следующий. Система устанавливается у провайдера и отслеживает сообщения электронной почты, удовлетворяющие какому-либо критерию (адрес получателя, отправителя). Для использования этой системы в деятельности по борьбе с преступностью, в том числе оборотом оружия, наркотиков, терроризмом требуется решение суда в каждом конкретном случае, так как происходит нарушение прав граждан на тайну личной информации. Однако проверить правомерность такого использования практически не представляется возможным, так как доступ к ней, а также информацию о ее параметрах и характеристиках имеют только сотрудники ФБР. Это обусловливает возможность применения системы «Хищник» в том числе для контроля проходящей через США информации в ущерб другим странам.

Контроль за информацией в сетях связи является относительно пассивной мерой, однако иностранными государствами разрабатываются и средства активного поиска информации в открытых телекоммуникационных сетях. Речь идет о так называемых программах-агентах. Эти программы способны автономно существовать в компьютерной сети, внедряться в различное программное обеспечение, перемещаться по сети и собирать информацию, отвечающую определенным признакам. Отобранные материалы пересылаются программой по определенному электронному адресу, который является анонимным почтовым ящиком. Преимуществами данных программ являются относительная дешевизна их разработки и использования, конспиративность и непрерывность сбора информации.

Кроме того, иностранными спецслужбами для добывания разведывательной информации активно используются хакеры. Спецслужбы США, в частности ФБР, используют хакеров не только из числа американских граждан, но и активно задействуют в своих операциях лиц из других государств. Об этом говорит факт разоблачения российской контрразведкой весной 2001 г. агента Федерального бюро расследований «Верса», которому было дано задание создать хакерскую группу для выполнения заданий ФБР, в частности для проникновения в компьютерные сети ФСБ России.

Но с помощью компьютерных сетей можно не только получать информацию, но и внедрять средства скрытого информационного воздействия для модификации и уничтожения данных, изменения программ и алгоритмов работы аппаратных средств, распространять, в том числе направленно, дезинформирующие материалы. В этих целях

используется такой вид информационного оружия, как компьютерные вирусы, то есть специально написанные компьютерные программы, обладающие способностью создавать свои дубликаты, внедрять их в вычислительные сети, файлы, системные области и иные выполняемые объекты[8]. Борьба с вирусами осложняется их многообразием, скоростью и масштабами распространения. Особую озабоченность вызывают вирусные программы, осуществляющие сбор информации с «зараженных» ими информационных систем и последующую ее передачу по каналам открытых телекоммуникационных сетей в заранее обусловленные адреса. Это становится возможным благодаря тому, что подавляющее большинство современного программного обеспечения разработано в США.

Серьезную угрозу для развивающейся российской информационной инфраструктуры может представлять кибервойна. Способы и методы, применяемые при ведении кибервойны, дают возможность задействовать для агрессии малые силы и средства (включая небольшие мобильные группы), которые децентрализованы (территориально рассредоточены) и тщательно замаскированы, что существенно затрудняет их обнаружение и уничтожение. Исследования в этой области активно проводят США, КНР, ряд других стран Запада, а также Азиатско-Тихоокеанского региона.

В условиях мирного времени «мягкие» акции — лучший инструмент для скрытного управления мировыми процессами. Некоторые из методов проведения подобных акций хорошо отработаны. В их арсенал входят традиционные средства информационно-психологического воздействия, не раз испытанные на гражданах бывшего Советского Союза, в том числе и США, и доказавшие свою эффективность.

[8] См.: Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. М., СК Пресс, 1998, с.13-16.

ГЛАВА 5. МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПЕРЕГОВОРНЫЙ ПРОЦЕСС

Несмотря на энергичные разработки разнообразных теоретических построений в области ведения информационной войны, не следует ожидать их обязательного воплощения в жизнь в ближайшем будущем. Причина этого состоит в том, что государственные и военные институты являются довольно консервативными структурами, и прохождение даже перспективной идеи от концептуальной разработки до практического воплощения подчас занимает десятилетия. Но даже теоретическая возможность ведения подобных войн не должна оставаться за скобками при обсуждении проблем национальной безопасности государства и не может игнорироваться при анализе политических процессов и подготовке к возможным конфликтам будущего. Возникающие при этом опасности и угрозы в сфере информационной безопасности требуют принятия не только практических шагов по созданию адекватных средств ведения информационной войны (как оборонительного, так и наступательного характера) и разработке методов их применения, но и дипломатических усилий, способствующих укреплению стратегической стабильности на основе совершенствования международного сотрудничества в этой сфере.

Информационная война для дипломатов и политиков является все еще новым явлением. Практическая реализация присущих ей средств и методов до сих пор многими признается, в лучшем случае, в частных проявлениях, например использование сети интернет в качестве среды ведения пропагандистской деятельности или использование графитовых бомб против объектов энергетической инфраструктуры в Югославии. Однако в основном все согласны, что уже в не столь отдаленном будущем велика вероятность неконтролируемого роста возможностей ведения информационной войны, развития и распространения соответствующих средств, что может привести не только к возобновлению гонки вооружений на качественно новом технологическом уровне и в принципиально новом стратегическом контексте, но и явиться поводом для развязывания (в качестве ответа на нетрадиционный вызов) вооруженных конфликтов с применением традиционных средств ведения войны.

В соответствии со спецификой развития различных стран на первый план для них выдвигаются различные аспекты информационной войны. Например, в США на уровне государственных позиций наблюдается устойчивая тенденция рассматривать в качестве информационной войны

исключительно действия против информационных инфраструктур (в узком понимании — информационных сетей). При этом рассматриваются преимущественно террористические и криминальные действия, в тех их аспектах, которые направлены против информационных систем и ресурсов[1]. В то же время в ряде стран «третьего мира», прежде всего на Ближнем Востоке, превалирует взгляд на информационную войну как совокупность пропагандистских действий, затрагивающих культурный и мировоззренческий уровень, с использованием информационных возможностей, предоставляемых процессами глобализации и общедоступностью СМИ. Две эти точки зрения, безусловно, являются полярными и не отражают всего спектра взглядов на информационную войну даже в упомянутых странах, однако они дают наглядное представление о существенных различиях в восприятии структуры рисков, возникающих в связи с развитием информационных технологий.

Несмотря на явные различия во взглядах на информационную войну и оценке спектра возникающих угроз национальной безопасности, практически все страны ясно осознают необходимость ведения международного обсуждения проблем информационной безопасности и информационной войны.

Международное право и информационная война

В настоящее время аналитики различных стран сходятся во мнении, что большая часть традиционных видов боевых действий включает в себя в том или ином виде отдельные аспекты «информационной войны» и прежде всего физические атаки на информационные системы с использованием традиционных видов оружия, психологические операции, дезинформацию, традиционные направления электронной борьбы (например, радиоэлектронное подавление приемопередающих и иных электронных систем). Наряду с этим в последние годы появились и такие виды оружия, которые в равной степени могут быть причислены как к информационным, так и к традиционным (взрывные генераторы электромагнитного импульса, высокомощные микроволновые устройства, орбитальное лазерное оружие, графитовые бомбы и т.п.), к которым, однако, достаточно просто могут быть применены уже разработанные нормы международного права и общепризнанные законы и обычаи ведения войны.

[1] Эта позиция нашла отражение в их инициативах в ООН (резолюция, принятая 55-й сессией Генеральной Ассамблеи на основе американского проекта приведена в Приложении 4) и деятельности в рамках G-8.

Следует оговориться, что конкретные новые виды такого оружия могут и не учитываться существующими договорами по контролю за вооружениями, однако в любом случае они относятся к числу средств, предназначенных для использования в военное время, и на них распространяются соответствующие международные нормы и требования.

Несколько иная ситуация складывается с собственно информационными операциями, в которых применяются методы и средства, не предусматривающие непременно разрушения физических компонентов информационных систем. Одним из основных видов таких операций являются «сетевые атаки», в ходе которых один из противников пытается получить нелегальный доступ к информационным ресурсам другого государства, в частности для разрушения, изъятия или искажения находящейся на них информации. Такие атаки чаще всего являются средством «хакерской борьбы», однако могут принимать и гораздо более изощренную форму, когда коммуникационные возможности глобальных сетей будут использоваться для ведения психологической борьбы на уровне национального самосознания (а не против вооруженных сил противника). И хотя для международного права вопрос о средствах, которыми проводится подобная информационная операция, носит в общем-то подчиненное значение, применение традиционных международных норм по отношению к возникающим в этом случае вопросам информационной безопасности будет в значительной степени затруднено. Поэтому видится обоснованным мнение о целесообразности создания общепризнанной системы оценок масштаба и уровня опасности информационных атак, которые определяли бы степень допустимых контрмер: от принятия международных санкций и политического давления до проведения силовых операций и начала военных действий против установленного агрессора.

Отметим, что согласно опубликованному в 1999 г. (и в новой редакции переизданному год спустя) Министерством обороны США документу под названием: «Оценки международно-правовых вопросов информационных операций»[2], ответ на кибернападение на Соединенные Штаты будет весьма решительным, а вероятные последствия широкомасштабной «сетевой атаки» оправдывают осуществление полномасштабного военного противодействия.

[2] An Assessment of International Legal Issues in Information Operations. US Army, 2000.

Наибольшие дискуссии вызывает вопрос «является ли атака на сетевые и информационные ресурсы государства военным актом?» Интересно мнение экспертов Министерства обороны США, что само понятие «военного акта» в значительной степени устарело, и более того, оно не упоминается в Уставе ООН и редко употребляется в современном дипломатическом языке. С учетом теории, военный акт представляет собой нарушение прав другой нации, определяемых международным законодательством, в результате которого жертва нападения объявляет войну своему противнику. При этом следует отметить, что международно-правовые аспекты акта объявления войны сами стали предметом обсуждения, причем согласно позиции Министерства обороны США концепция «военного акта» не играет никакой роли в современной международной правовой системе, санкции с применением военной силы могут последовать за значительно менее серьезным нарушением прав другой нации, и не будут рассматриваться как акт войны.

Аналогичная ситуация наблюдается и в отношении требований, выдвигаемых Уставом ООН и Декларацией принципов международного права о дружественных отношениях и сотрудничестве между государствами (Резолюция Генеральной Ассамблеи (ГА) ООН 26/25 от 1970 г.). Так, согласно статье 2(4) Устава ООН, члены этой организации берут на себя обязательство «воздерживаться от угрозы применения силы против территориальной целостности и политической независимости любого государства или любых других действий, несовместимых с целями ООН». В свою очередь, в Резолюции ГА ООН 26/25 и в Резолюции ГА ООН 33/14 (1974 г.) «Определение агрессии» были сформулированы основные критерии агрессии, и она определяется как преступление, за которое международным правом предусматривается ответственность. Наконец, статья 51 Устава ООН предусматривает правомерность использования индивидуальной или коллективной самозащиты только в том случае, если против них было совершено вооруженное нападение. Таким образом, если проведение информационной операции не будет признано вооруженным нападением или «актом войны», может оказаться, что право самозащиты от информационных атак также не будет признаваться законным с точки зрения международного права.

Позиция Соединенных Штатов по этому вопросу сводится к тому, что они вообще стремятся рассматривать декларации Совета Безопасности и других органов ООН исключительно в качестве рекомендаций. В особой мере это касается упомянутой выше резолюции «Определение агрессии». После ее принятия на сессии ГА ООН американская делегация выразила

мнение, отражающее позицию правительства США, что данная декларация не устанавливает прав и обязанностей государств, а может всего лишь «служить полезным руководством» для Совета Безопасности. После бомбардировок американской авиацией Ирака в 1998-1999 гг. и проведения воздушной кампании НАТО против Югославии в 1999 г. принципы определения агрессии представляются еще более размытыми.

Нельзя также не упомянуть и о том, что в США находит распространение еще более радикальная точка зрения на отношения с ООН, достаточно четко сформулированная вице-президентом влиятельной консервативной американской организации «Фонд наследия» К. Холмсом в 1998 г. в программном документе «Внешнеполитические вызовы. Консервативная доктрина»[3]. В нем, в частности, предлагается строить внешнюю политику США по более конфронтационному по отношению к международным организациям сценарию. Так, согласно Холмсу, США должны устранить контроль над своей внешней политикой со стороны ООН. Он критикует в целом достаточно агрессивную политику клинтоновской администрации за адаптацию внешнеполитической доктрины США к требованиям ООН и других международных организаций. В тех случаях, когда интересы ООН вступают в противоречие с интересами США, Холмс предлагает избирать самостоятельный курс, даже если в этом случае им придется действовать в одиночестве, оставляя тем самым за собой право действовать независимо от постановлений Совета безопасности ООН. Кроме того, США должны настаивать на реформировании ООН, а также отказываться от любых платежей и взносов в эту организацию, если будут отвергаться привилегии США по голосованию в ней.

Эксперты Министерства обороны США неоднократно выступали с критикой намерения мирового сообщества увязать информационные атаки с понятиями «вооруженного нападения» и «применения силы»[4]. Интересно отметить, что европейские специалисты явно расходятся во взглядах по этому вопросу с американскими экспертами. В частности, О. Брингманн, в течение ряда лет проводивший изучение данной проблемы по заказам военных ведомств ФРГ и Нидерландов, прямо

[3] Ряд положений данного документа находит реальное отражение во внешней и военной политике США. Это касается, в частности, энергично отстаиваемой руководством этой организации позиции по вопросу о создании национальной системы противоракетной обороны и возможности выхода США из Договора по ПРО от 1972 г.

[4] Хотя такой подход в некоторой мере даже обостряет проблему определения информационных атак, поскольку требует одновременно определить информационное оружие как инструмент проведения «вооруженного нападения», тем не менее он, по всей видимости, позволит определить порог использования информационных атак в качестве законного средства воздействия по мандату ООН в случае «возникновения угроз миру».

говорит о возможности определения наступательных информационных операций как акта агрессии и, соответственно, считать законным принятие адекватных ответных действий[5].

Все установленные международно-правовые принципы, касающиеся таких понятий, как «применение силы», «акт агрессии», «вооруженное нападение» или «акт войны», сходятся в том, что предусматривают наличие оружия и его применение. Иными словами, все они вступают в силу, когда появляется особая угроза, возникающая от применения оружия, в частности, вооруженное нападение предусматривает определенный уровень физических разрушений и/или захвата территории государства, по отношению к которому было совершено нападение. Отечественное определение оружия как «устройств и средств, предназначенных для поражения противника в вооруженной борьбе»[6] или «всякого средства, приспособленного, технически пригодного для нападения и защиты, а также совокупность таких средств»[7], является достаточно общим и естественным образом включает в себя и средства информационного воздействия. Однако те или иные национальные определения конкретных понятий и категорий не могут ограничивать международное право.

Возвращаясь к приведенному выше определению вооруженного нападения, следует отметить, что оно не в полной мере учитывает характеристики тех средств и видов силового воздействия, которые уже признаны мировым сообществом в качестве оружия, но непосредственно не подпадают под данное определение. Например, химическое и бактериологическое оружие практически не наносят никакого физического ущерба и не уничтожают физические объекты — они предназначены только для поражения живой силы (человека) или элементов биосферы. Более того, ослепляющие лазерные системы, генераторы инфразвука и другие виды так называемого «нелетального оружия» вообще лишь на время выводят из строя человека и, тем не менее, признаны в качестве оружия. Исходя из этого, международное право при определении понятий «оружия» и «вооруженного нападения», видимо, должно ориентироваться на совершенно иные критерии, в частности, важно не то, какое действие (разрушающее, инкапаситирующее или другое) оказывает тот или иной вид оружия, а то, какие цели преследует использующая его сторона. В соответствии с этим

[5] Bringmann O. Information Operations — Legal Aspects. Briefing. Germany.
[6] Военный энциклопедический словарь. М., Военное издательство, 1983, с.523.
[7] Ожегов С.И. Словарь русского языка. М., Русский язык, 1985, с.394.

в самом общем виде оружие можно было бы определить как средство достижения военного превосходства над противником, способное, если это необходимо, вызывать разрушения. Исходя из этого расширенного определения оружия, проведение атак, предпринимаемых каким-либо государством против информационной инфраструктуры другого государства, а также проведение других информационных операций могут и должны рассматриваться в качестве вооруженного нападения.

В этом случае, особенно если последствия проведения информационной операции оказываются сопоставимыми с последствиями применения обычных видов вооружения, следует признать законным (с международно-правовой точки зрения) право государства на самозащиту. При этом может допускаться проведение не только ответной информационной операции, но и традиционных военных действий (при условии соблюдения принципов необходимости и пропорциональности). Такой подход, в свою очередь, вызывает необходимость решения ряда новых вопросов, к числу которых следует отнести определение порогового уровня информационных атак, после достижения которого становятся допустимыми ответные действия, обоснование оправданности и пропорциональности, принципы идентификация агрессора, а также возможность действий против третьей страны, с территории которой осуществляется информационная операция. На практике выявление стороны-агрессора является наиболее трудной задачей.

В то же время явно прослеживается стремление перевести информационные атаки в разряд террористических действий, а проблему противодействия «сетевым атакам» решать в рамках антитеррористической борьбы. Определяя информационные атаки как террористический акт (что в значительной степени облегчается тем, что такие атаки, как правило, проводятся в условиях анонимности), США фактически резервируют за собой право проведения асимметричной ответной операции, в том числе и с использованием традиционных силовых методов. Одновременно они пытаются оправдать наличие наступательных возможностей проведения информационных операций стремлением обеспечить собственные права и защиту от потенциальной агрессии.

В этой связи любопытным представляется мнение экспертов Министерства обороны США[8] относительно возможных ответных действий со стороны государства, подвергшегося информационной атаке.

[8] An Assessment of International Legal Issues in Information Operations. US Army, 2000.

В упомянутых выше «Оценках международно-правовых вопросов информационных операций» высказывается точка зрения, что если анонимная информационная атака может быть достоверно идентифицирована как спланированная и проведенная другим государством акция, то потерпевшая сторона будет иметь право опротестовать их и, возможно, инициировать разбор сложившейся ситуации на слушаниях в международной организации. И только в случае, если международное сообщество убедится, что такая атака или серия атак могут рассматриваться как «вооруженное нападение», пострадавшему государству следует предоставить право проведения ответных действий, как путем проведения встречной информационной операции («сетевой атаки»), так и традиционными силовыми действиями.

Здесь наблюдается явная противоречивость американской позиции по вопросу правомерности проведения информационных атак. С одной стороны, как уже отмечалось, США резервируют за собой право проведения информационных операций в качестве «смягченных» санкций, предусмотренных международным правом, или же в качестве «гуманного» средства предотвращения агрессии. С другой стороны, принимая во внимание угрозу проведения атак против собственных информационных систем, США стремятся определить их как террористические действий, т.е. поставить «вне закона». В соответствии с этим национальное военное руководство США может принять решение о проведении ответной информационной атаки против систем другого государства даже несмотря на то, что право на самооборону не может в полной мере оправдывать действия «активной обороны», в случае если информационная атака проводится террористической организацией или отдельным лицом с территории другого государства, и это государство не в состоянии остановить эти действия, а санкции, предпринимаемые международными организациями, оказываются недейственными.

Существуют и иные подходы к проблеме международно-правовой квалификации информационных операций. Возможно, например, провести разделение между информационными операциями, направленными против собственно информационных инфраструктур, и специальными операциями, такими как дезинформация населения, оказание давления через СМИ и т.п. При этом следует иметь в виду, что информационные операции, проводимые против информационных систем отдельного государства, могут также оказывать влияние и на международные информационные инфраструктуры в целом, а последние находятся под защитой ряда международных соглашений, например,

Соглашения о международном телекоммуникационном сообществе[9]. При этом важным моментом является то, что большинство заключенных к настоящему времени соглашений распространяются как на страны-участницы, так и на третью сторону, которая использует находящиеся под защитой объекты. В большинстве случаев стороны обязуются не использовать международные информационные системы в военных целях.

Практически все члены международного сообщества признают необходимость определить и согласовать на международном уровне перечень ключевых информационных систем (как государственных, так и не государственных), функционирование которых является критически важным для обеспечения жизнедеятельности и национальной безопасности государств. Выделение такого класса информационных систем позволит определить по отношению к ним повышенные меры защиты, включая правомочность принятия ответных мер («активной обороны») в случае проведения против них информационных операций. Это позволит также выработать экстренные механизмы международного реагирования на угрозы в информационной сфере, учитывающие степень их воздействия на национальную безопасность различных стран.

Еще одна важная проблема, требующая обсуждения на международном уровне, касается использования в мирное время информационной операции (на уровне существенно ниже, чем вооруженное нападение) как инструмента государственных санкций или вмешательства[10]. В соответствии с правом, в случае нарушения прав нации, находящихся под защитой международного права, предусматриваются пропорциональные ответные действия потерпевшего государства, если они не направлены на провокацию использования военной силы. Среди таких контрмер могут рассматриваться: разрыв дипломатических отношений, торговое и транспортное эмбарго, отказ от оказания помощи, блокирование банковских активов, принадлежащих другой нации и т.д. Однако звучат предложения отнести к числу таких действий также и введение ограничений на информационные возможности «страны-нарушителя». В

[9] Вычленение национальной составляющей глобальной инфраструктуры, необходимое, в частности, для обеспечения ее защиты международным правом, представляется уже в настоящее время весьма затруднительным, поскольку требует определения и перечисления многочисленных параметров и, кроме того, позволяет чрезмерно широко трактовать само это понятие. Поэтому вмешательство в работоспособность информационных систем государства, затрагивающее также работоспособность международных и глобальных систем, должно быть признано незаконным. Наиболее логичным в этих условиях выглядит принятие международной конвенции, дающей «кибернетическому (информационному) пространству» статус зоны международной защиты, по аналогии с космическим пространством и открытым морем, а также определение глобальных информационных систем, как «демилитаризованной зоны».

[10] Как часть информационного противоборства.

случае их принятия, если принцип введения международного эмбарго будет распространен на информационную сферу, тот, кто будет контролировать рынок коммуникационных и информационных услуг в мире (в том числе в экономической сфере), будет фактическим монополистом в части использования и этого инструмента.

Однако существуют обстоятельства, препятствующие такому развитию событий. В частности, международное право запрещает вмешательство во внутренние дела государств, понимая под ним все виды воздействия, которые может предпринимать одно государство против другого, используя «давление» с намерением изменить или подавить возможности его свободного волеизъявления. В то же время Устав ООН не предусматривает самообороны с использованием вооруженных сил или оружия в качестве ответа на такое вмешательство.

Если будет принята расширенная трактовка понятия «оружия» и информационная среда станет зоной, защищенной международным правом, а также в случае, если асимметричные действия, направленные против другого государства в информационной сфере, затрагивают функционирование его жизненно важных информационных систем, подобные действия можно будет квалифицировать не как экономическое или дипломатическое давление, а как вооруженное нападение, что предоставит противоположной стороне право на применение мер самозащиты.

Международно-правовое регулирование информационного противоборства

Как уже отмечалось, современная стратегия ведения боевых действий в ходе вооруженного конфликта предусматривает применение различных технических средств (комплексов и систем оружия), которые, так или иначе, ассоциируются с понятием «информационного оружия». Наиболее известными примерами такой техники являются системы радиоэлектронного противодействия, аппаратура связи и технической разведки. В ближайшей перспективе можно ожидать дальнейшего повышения значимости мероприятий по обеспечению защиты линий связи и информационных систем, используемых в военных целях. Особое значение при этом приобретает тот факт, что подобные информационные системы становятся все более тесно сопряженными как с гражданской информационной инфраструктурой государства, так и с системами, находящимися в международном пользовании.

Вместе с тем следует отметить, что существующие международные договоры, призванные ограничить распространение тех или иных видов оружия, далеко не всегда учитывают факт существования такого информационного оружия, хотя выведение из строя подобных систем, особенно на начальной стадии развития конфликта, относится вооруженными силами большинства стран мира к числу приоритетных боевых задач.

Исходя из вышесказанного, при анализе проблемы международного регулирования военных аспектов информационной безопасности, представляется целесообразным в первую очередь рассмотреть два основных аспекта: вопросы применимости к информационным войнам международно-правового регулирования правил ведения войны и возможность начала переговорного процесса в области ограничения информационных видов оружия.

Правила ведения вооруженного конфликта и информационная война

Вопросы применимости законов и обычаев ведения войны к информационным операциям часто поднимаются в работах западных, прежде всего, американских специалистов в области информационного противоборства. Это обсуждение носит принципиальный характер, и от его результатов во многом будет зависеть стратегия военного строительства большинства стран мира.

Прежде всего следует отметить имеющее место у некоторых «экспертов» стремление к пересмотру основополагающих принципов международного права, например, замене термина «законы и обычаи ведения войны» на «правила ведения вооруженного конфликта». Это связывается с тем, что в настоящее время государства редко объявляют войну, но часто оказываются вовлеченными в более или менее крупные вооруженные конфликты. Однако при этом сам термин «международный вооруженный конфликт» оказывается за рамками определений, предусмотренных Гаагскими и Женевскими конвенциями и другими международными соглашениями. Поэтому такая подмена понятий создает опасный прецедент, поскольку государства, избегая акта объявления войны, сталкиваются с невозможностью проведения четкой грани между окончанием политической фазы развития конфликта и началом военной[11].

[11]По мнению экспертов Министерства обороны США, «в настоящее время в международном праве не существует никаких ограничителей на проведение информационных операций. [...] Развитие международного права в этой области будет в значительной мере тем, что будут говорить и делать в кризисные моменты лица, принимающие решения. (An Assessment of International Legal Issues in Information Operations, March 1999).

Это обстоятельство особенно важно в связи с тем, что в последние годы постоянно предлагаются все новые понятия (конфликты низкой интенсивности, операции, отличные от войны, государства-«изгои», гуманитарные интервенции), многие из которых практически не поддаются четкому определению. Не стремятся ли их авторы тем самым легитимизировать собственные силовые действия, добиваясь возможности их проведения без какого бы то ни было участия международных институтов?

Однако такая позиция имеет и оборотную сторону. Например, если не определить информационную атаку как акт агрессии, те же США, обладая наиболее развитой и уязвимой информационной инфраструктурой, могут оказаться жертвой подобных действий (в отношении криминальных атак именно это и имеет место). Арбитраж мирового сообщества в разрешении такого конфликта становится вообще невозможным, т.к. он сводится к банальной разборке («кто начал первым») без опоры на четкие, всемирно признанные критерии. Если же информационные атаки будут признаны вооруженными действиями, то на них должны распространяться основные законы и обычаи ведения войны, однако подмена термина «война» термином «международный вооруженный конфликт» вообще может вернуть ситуацию на начальный уровень обсуждения.

Принцип военной необходимости

Согласно одному из распространенных определений, разрешается использование силы, не запрещенной законами и обычаями ведения войны, с контролируемой степенью, необходимой для частичного или полного подчинения противника с минимальным уровнем потерь людей, времени и ресурсов. В другой трактовке этого понятия говорится о «мерах, необходимых для обеспечения окончания войны и являющихся законными с точки зрения законов и обычаев ведения войны».

Так или иначе, все известные трактовки данного принципа сходятся в том, что в ходе войны вооруженная сила должна применяться избирательно. Вследствие этого некоторые виды информационного оружия, прежде всего такие, как компьютерные вирусы, «троянские кони», логические бомбы и прочие программные и аппаратные средства, разрушающие информационные системы и не обладающие свойством избирательного действия, не могут считаться законным средством ведения (информационной) войны. Они должны быть причислены, в зависимости от масштабов возможных последствий, либо к средствам ведения

террористической борьбы, либо к ОМУ, а разработка таких видов воздействия на государственном уровне должна регламентироваться соответствующими нормами международного права.

Данное положение, в свете постоянно появляющихся сообщений о создании, в частности в КНР и Тайване «боевых вирусов», которые могут быть применены ими (а по некоторым сообщениям, уже применяются в ограниченных масштабах[12]) друг против друга в случае начала конфликта, имеет уже не только теоретический, но и практический интерес. В случае распространения принципа военной необходимости на сферу информационного противоборства, независимо от реальной возможности создания «боевых вирусов» можно говорить о поддержке, например, Тайванем терроризма или о создании им ОМУ. Вопрос усложняется тем, что, являясь сравнительно новым видом боевых действий, информационные операции подпадают под исключение из этого определения («использование силы, не запрещенной законами и обычаями ведения войны»), что заводило в тупик обсуждение проблемы еще до осмысления категории информационного оружия и тактики ведения информационной войны.

Таким образом, согласно существующим нормам международного права, разработка, создание и принятие на вооружение ряда видов информационного оружия (не обладающих избирательностью действия) не могут быть в настоящее время поставлены под контроль, хотя многие страны осознают настоятельную необходимость заключения договоров в этой сфере.

Сложнее обстоит дело с информационным оружием, обладающим избирательным действием, в частности (абстрагируясь от конкретных средств ведения информационной войны) предназначенным для использования против категории объектов информационной инфраструктуры, являющихся «законными целями», например военных информационных систем.

С одной стороны, принцип военной необходимости (в отношении информационных операций) работает на сторонников их более широкого применения, выдвигающих в качестве аргументов в пользу информационных операций именно их гуманность, поскольку они, как правило, направлены против технических (программных) компонентов информационных систем и обладают качеством «нелетального» оружия, а

[12]Stanton J.J. Rules of Cyber War Battle U.S. Government Agencies. National Defense, February 2000, p.29.

также краткосрочность их проведения и возможность достижения желаемого результата без физического уничтожения ресурсов противника. Вместе с тем полное разрушение в результате таких операций информационной и телекоммуникационной инфраструктуры государства, как того требуют часто выдвигаемые американскими специалистами требования к стратегии ведения информационной войны[13], способно вызвать паралич экономической системы, нарушение управления авиаперевозками, а также нарушение энергетической системы. С уверенностью можно говорить о том, что такие масштабные разрушения информационной инфраструктуры государства неизбежно повлекут за собой гибель гражданских лиц, которая не может быть оправдана военной необходимостью. Это подтверждает, в частности, практика проведения воздушной операции НАТО в Югославии, которая действительно привела к значительным физическим разрушениям и жертвам среди гражданского населения, не понизив в сколько-нибудь значительной степени возможности военного сопротивления со стороны Югославии.

Таким образом, требование нанесения максимального ущерба информационной структуре государства противоречат принципу военной необходимости. Кроме того, они вступают в явное противоречие с существующими международными договоренностями (такими как INTELSAT и IMARSAT), а также с положениями ряда международных соглашений, касающихся соблюдения прав нейтральной стороны.

Следует упомянуть и другую проблему, связанную с применением принципа военной необходимости к информационным операциям, которая заключается в сложности разделения собственно военных и гражданских информационных систем. Так, в США более 95% военных коммуникаций пересекаются, а то и непосредственно ориентируются или базируются на гражданских объектах информационной инфраструктуры. Поражение военных объектов может быть оправдано военной необходимостью, однако при этом нельзя исключить нанесения существенного урона и гражданским системам. США, таким образом, сталкиваются с дилеммой, создаваемой асимметрией проведения

[13]Здесь следует обратить внимание на то, что еще в 1994 г. полковник ВВС США О. Иенсен в статье «Информационная война: принципы войны третьего поколения» следующим образом формулирует ее задачи: «Необходимо нарушение или уничтожение телефонных, радио, кабельных и иных средств передачи информации противника. Разрушьте нервную систему. Нарушьте, прервите, понизьте возможности или уничтожьте любую передачу данных. Не оставляйте никаких лазеек. Перекройте доступ противника к спутникам связи третьих стран, независимо от того принадлежат они международным консорциумам, коммерческим компаниям или не вовлеченным в конфликт странам». Jensen Owen E. Information warfare: principles of third world war. *Airpower Journal*, winter 1994, pp.35-44.

собственных наступательных и оборонительных информационных операций, что может быть использовано при обсуждении вопросов информационной безопасности на переговорах различного уровня.

Решение этой дилеммы может лежать в последовательном применении следующего принципа.

Принцип гуманности
В соответствии с этим принципом запрещается использование любой силы, независимо от ее степени, в том случае, если она не служит достижению целей войны, которыми являются частичное или полное подчинение противника с минимальным уровнем потерь людей, времени и ресурсов.

Этот принцип является зеркальным отражением предыдущего принципа («военной необходимости»), и именно он чаще всего используется активными сторонниками ведения информационной войны в качестве ее легального оправдания. Действительно, при ведении информационных операций, независимо от их конкретной формы, человеческая жизнь подвергается опасности только косвенно. Иными словами, непосредственными целями являются информационные системы, информационные потоки или непосредственно сознание человека, но не его жизнь.

Тем не менее на данную проблему можно посмотреть и с другой стороны. В частности, если установлено, что информационная атака являлась террористическим актом со стороны какой-либо не связанной с государством группы, то в этом случае проведение ответной полномасштабной информационной операции (которая может нанести ущерб информационным ресурсам государства, с территории которого проводился террористический акт, или вызвать более серьезные последствия) вряд ли удовлетворяет принципам «гуманности».

При планировании и проведении информационных операций, независимо от их конкретных методов, должна предусматриваться «пропорциональность» ущерба, наносимого гражданским и военным объектам, т.е. должны учитываться как требования международного права в части использования силы (когда идет речь об определении необходимого уровня использования силы при проведении ответных действий), так и требования принципов ведения войны. В любом случае, лицо, принимающее решение о проведении той или иной операции (в том числе

и информационной) должно исходить из необходимости максимально возможного уменьшения жертв среди гражданского населения.

С точки зрения гуманитарного права, как справедливо отмечают Л. Гринберг, С. Гудмен и К. Су Ху, оценка «легальности» операций должна производиться, исходя из приносимого ей ущерба для гражданского населения, а не из методов и средств, с помощью которых она проводилась[14]. Иными словами, косвенный ущерб, наносимый информационными атаками, например, авиакатастрофы в случае паралича диспетчерских служб, также должен учитываться в качестве аргумента против информационных атак даже узкой направленности.

Как уже отмечалось, военные информационные системы тесно переплетаются с гражданскими, поэтому атаки, направленные против военных целей, могут вызвать нарушения работоспособности связанных с ними гражданских систем, а поражение гражданских систем ведет к снижению военных возможностей государства. Вследствие этого в ряде случаев американские эксперты используют общую систему аргументации для оправдания двух диаметрально противоположных позиций, защищаемых ими в зависимости от целей, которые они перед собой ставят: обоснование правомочности нанесения удара по гражданским объектам противника или отнесение собственных военных систем к категории объектов, находящихся под защитой международного права.

Однако существуют принципиальные различия между этими позициями. Если информационная операция проводится в военное время непосредственно против одного из элементов военной системы противника и влечет за собой побочные разрушения связанных с этими элементами гражданских систем и объектов, то ответственность за это должна нести сторона, использующая такие информационные системы «двойного назначения». В качестве аналогии здесь можно указать на использование обороняющейся стороной заложников в качестве «живого щита» от нападения. Если же непосредственной целью такой информационной атаки является гражданская система (непосредственно не связанная с системами военного назначения), то ответственность следует возложить на сторону, проводящую атаку, а сами эти действия должны рассматриваться как нарушение основополагающих норм международного права.

[14]Greenberg Lawrence T., Goodman Seymour E., Soo Hoo Kevin J. Information Warfare and International Law. National Defense University Press.

Аналогичным образом необходимо поставить вне закона использование международных систем в качестве средства или среды для проведения информационной операции и другой военной активности. Такая постановка вопроса, способствующая концентрации ответных действий на государстве-нарушителе, будет эффективно противодействовать применению силы непосредственно против международных систем.

В случае принятия международным сообществом правомочности таких принципов проведения информационной операции, возникает настоятельная необходимость формирования перечня гражданских и транснациональных объектов, защищаемых международным правом, а также военных систем, атаки против которых будут носить законный характер.

Рассмотренная выше аргументация касалась действий, проводимых против информационных систем, при этом вне рамок обсуждения оставался, по-видимому, не менее важный вопрос манипуляции сознанием противника. В принципе такие действия мало соотносятся с законами и обычаями ведения войны. Вместе с тем многие западные эксперты полагают, что использование ряда социальных технологий, дезинформация на высшем политическом уровне и проведение пропагандистских кампаний в стране-противнике (актуальном или потенциальном), формирование образа противника в мире может оказывать существенное, если не решающее воздействие на военные возможности противника. По мнению полковника ВВС США Р. Шафрански, понятие «информационная война» вообще целесообразно свести именно к таким действиям.

Л. Гринберг, С. Гудмен и К. Су Ху в работе «Информационная война и международное право» утверждают, что манипулирование сознанием противника может инициировать внутренние беспорядки или даже послужить непосредственной причиной актов геноцида и других тяжелейших преступлений. И в настоящее время такая возможность приобретает практический характер, в обоснование чего приводится деятельность так называемого «радио ненависти», внесшего свой вклад в разжигание межэтнических конфликтов и геноцида в Руанде и бывшей Югославии. По мнению этих американских аналитиков, пропаганда и вводящие в заблуждение радиовещательные и телевизионные программы (дезинформация), способствующие развязыванию гражданской войны или геноциду, должны считаться незаконными.

Аналогичные ограничения должны распространяться на ведение дезинформации в ходе военных действий. Уловки, дезинформация, маскировка и тому подобные меры, безусловно, допустимы на войне, например, некоторые военные уловки, призванные ввести в заблуждение противника, заставить его совершать опрометчивые поступки или направлять его действия по выгодному для себя сценарию могут считаться вполне законными. Но это относится далеко не ко всем видам военного обмана, что нашло свое отражение в ряде международных договоренностей.

В частности, к разряду запрещенных принято относить так называемые «вероломные» действия, призванные убедить противника в том, что собственные намерения и действия соответствуют нормам международного права и нормам ведения войны, в то время как они имеют целью обмануть полученное в результате доверие. Вероломные действия включают имитацию перемирия или сдачи, использование в военных целях гражданского или иного статуса, предоставляющего защиту в военный период, например, действия от лица нейтральной страны или международной организации. Запрещено также ношение униформы и использование иных опознавательных знаков противника.

Информационные операции, направленные на манипуляцию сознанием противника, также должны ограничиваться по аналогии с запрещением вероломных действий. Незаконными являются и попытки маскировать боевую технику под медицинский транспорт или под технику нейтральной стороны. По аналогии с этим следует считать незаконной манипуляцию информационными ресурсами противника, при которой искажения, вносимые в базы данных, используемые противником для планирования и проведения военных действий, приведут к тому, что военный объект будет принят за гражданский.

Следует особо отметить, что в настоящее время, в отличие от униформы и опознавательных знаков, системы связи и информационные системы не регламентируются положениями о вероломных действиях, хотя в ряде случаев использование коммуникационных и информационных систем в военной сфере может быть гораздо более действенным боевым средством, чем простое использование маскировки и дезинформации. Тем более что тактика, базирующаяся на вероломстве, практически всегда может быть более успешной, чем действия без использования новых технических средств. Американские специалисты, несмотря на существующее явное превосходство США в информационной сфере, уделяют этому вопросу

значительное внимание и, по-видимому, заинтересованы в его рассмотрении.

Международное право в области ограничения информационных видов оружия

Чрезвычайно широкое разнообразие трактовок термина «информационная война» и большинства ее аспектов не позволяет подробно проанализировать все существующие договоры и перспективы международного диалога в сфере информационной безопасности. Однако можно выделить несколько важнейших договоренностей, которые могут быть отнесены к вопросу проведения информационной операции.

Договор о космосе 1967 г.

Современные средства коммуникации и системы навигации немыслимы без использования космических спутников, в связи с чем анализ проблем информационной войны требует рассмотрения договоров, касающихся использования космического пространства.

В частности, Договор о принципах деятельности государств по исследованию космического пространства, включая Луну и другие небесные тела (известный также как Договор о космосе), содержит положение о том, что «государства-участники обязуются не размещать на околоземной орбите объекты, несущие ядерное оружие и другие виды оружия массового поражения...». Как известно, термин «оружие массового поражения» или «оружия массового уничтожения» чаще всего распространяется только на ядерное, химическое и биологическое оружие, и хотя эксперты все еще колеблются в вопросе о квалификации информационного оружия как ОМУ, многие из них тем не менее склонны рассматривать данное положение Договора о космосе в тесной увязке с вопросами ведения информационной войны. Вместе с тем очевидная трудность применения положений Договора к информационному оружию состоит в том, что он запрещает лишь размещение на орбитальных объектах ОМУ, в то время как искусственные спутники земли (ИСЗ) (например, спутники системы GPS) и другие космические аппараты могут использоваться в качестве ретрансляционных пунктов, обеспечивающих работу различных комплексов вооружений, в том числе ОМУ и информационного оружия.

Договор о космосе устанавливает также, что «Луна и другие космические объекты должны использоваться государствами-участниками Договора исключительно в мирных целях. [...] Испытания любого типа оружия и

проведение военных маневров на космических объектах должно быть запрещено». Здесь важно отметить, что согласно большинству трактовок термин «космические объекты» относится только к космическим телам естественного происхождения, таким как Луна, астероиды и планеты, и не распространяется на ИСЗ и другие космические аппараты. Таким образом, это положение Договора едва ли может служить ограничением на размещение информационного оружия в космосе.

Важным моментом Договора о космосе, а также других соглашений, относящихся к использованию космического пространства, является то, что они сходятся в одном: использование космоса допустимо только в мирных целях. Между тем системы INTELSAT-60 и INTELSAT-61, создававшиеся в мирных целях, могут использоваться и для проведения информационных операций. При этом возникает вопрос, может ли система рассматриваться как гражданская, если получаемая со спутников информация используется в военных целях? Ответа нет.

Таким образом, наряду с запрещением выведения в космос боевых компонентов (например, космических элементов систем ПРО), эксперты ставят под сомнение возможность разграничения военных и гражданских ИСЗ, которые также могут использоваться для информационного обеспечения боевых операций. Это, в свою очередь, создает правовую коллизию с договорами об использовании космического пространства. Данный вопрос тем более актуален, что некоторые современные системы вооружения могут применяться только в комплексе с космическими системами[15]. Более того, можно смело утверждать, что опосредованное использование в военных целях как космических систем, в частности, так и информационных систем в целом в будущем будет только возрастать.

Конвенция об обязательствах

Конвенция об обязательствах является еще одним международным соглашением, регламентирующим деятельность человека в космосе, и она в полной мере может быть применена к информационным операциям. Однако существенным ограничением здесь является то, что она касается, прежде всего, положения мирного времени и никоим образом не ограничивает развития космических информационных систем вооружений.

[15]Абстрагируясь от эффективности данного комплекса, отметим, что навигационное обеспечение и целеуказание бомбардировщика B-2 осуществляется исключительно с помощью космических систем. Однако соответствие его Договору о космосе никогда даже не ставилась под сомнение.

Статья 2 Конвенции об обязательствах гласит, что «страна, выводящая на орбиту спутник, гарантирует выплату компенсации в случае, если принадлежащий ей космический объект причиняет какой-либо ущерб на поверхности Земли либо самолетам в воздухе». Так как Конвенция вступила в силу в 1972 г., она не могла рассматриваться в качестве ограничителя военной информационной активности. Между тем определение термина «ущерб» (статья 1 Конвенции) не регламентирует способа причинения ущерба, а формулирует его как «потерю жизни, увечья или иное ухудшение здоровья, или потерю или повреждения, причиненные имуществу государств, или частного лица, или собственности международной, межправительственной организации».

Наиболее спорным в данном случае является вопрос, можно ли считать ущербом потерю, искажение или утечку информации? Если нет, то подпадают ли под действие данной Конвенции манипуляции с информационными ресурсами, проводимые посредством космических систем?

Международная телекоммуникационная конвенция

Разработка и создание информационных видов оружия может противоречить ряду положений Международной телекоммуникационной конвенции, в которой, в частности, утверждается, что «все приемо-передающие станции, независимо от их целей, должны устанавливаться и работать таким образом, чтобы не оказывать опасного воздействия на радиослужбы и коммуникации других членов конвенции...». В известной мере это соглашение накладывает ограничение даже на использование самолетов-постановщиков помех, чья аппаратура способна выводить из строя не только военные, но и гражданские радиоэлектронные средства. Однако в данном случае речь идет, во-первых, об использовании систем радиоэлектронного подавления в военное время, а во-вторых, воздействие на гражданские объекты, если таковое имеет место, не является непосредственной целью данных систем.

В то же время еще 21 августа 1995 г. американский журнал «Тайм» опубликовал статью под названием «Наступающие киберсолдаты», в которой говорилось о новейшем секретном проекте ВВС США, в рамках которого создавался специальный самолет «Команде Соло», предназначенный для подавления телевизионных и радиопередач страны-противника на любой частоте и одновременной замены оригинального вещания своим собственным. Между тем в статье 38 Международной телекоммуникационной конвенции говорится, что «участники

соглашаются предпринимать шаги для предотвращения передачи и циркуляции ложных сигналов бедствия, чрезвычайной ситуации, безопасности или идентификационных сигналов (позывных)». Таким образом, в данном случае речь идет о прямом нарушении телекоммуникационной конвенции.

Не менее важным представляется вопрос о том, являются ли нарушением конвенции действия, приводящие к физическому уничтожению гражданских приемо-передающих телевизионных и радиовещательных систем. Примером таких действий может служить воздушная кампания НАТО в Югославии, когда теле- и радиопередающие станции определялись в качестве приоритетных целей для поражения, а в качестве элементов ведения психологической борьбы разбрасывались миниатюрные радиоприемники, настроенные на фиксированную частоту пропагандистской станции НАТО.

Соглашения в области ограничения и сокращения вооружений

Проблема ограничения информационных видов оружия является одной из важнейших в сфере информационной безопасности, тем более что в настоящее время она не подпадает под действие ни одного из международных договоров в области ограничения и сокращения вооружений (за возможным исключением Договора по ПРО от 1972 г., в котором накладываются ограничения на строительство радиолокационных станций слежения). Более того, эта проблема, как правило, остается за рамками проводимых за рубежом научно-аналитических исследований, посвященных информационным войнам, в которых на первое место выступают чаще всего не военные аспекты, а проблемы информационного терроризма, распространения критических информационных технологий, психологического противоборства.

Так, например, наиболее активным сторонником перевода вопросов информационной безопасности в русло обсуждения проблем информационного терроризма являются США. Под тем же углом зрения склонно рассматривать данные вопросы и Министерство национальной обороны Южной Кореи, о чем, в частности, свидетельствует работа официального представителя Ли Суп Хо «Создание международной организации сотрудничества по защите от информационного терроризма»[16]. Следует отметить, что такая позиция вовсе не означает, что в указанных странах не ведутся работы по созданию информационных

[16]Sungkoo Lee. Constructing International Cooperative Organizations for Defending Information Terrorism. Ministry of National Defense, Seoul, Korea.

видов оружия. Однако она сигнализирует о стремлении вывести военный аспект обеспечения информационной безопасности из международного правового поля.

Существуют и другие позиции. Например, в работах индийского аналитика А. Джоши[17] прослеживается явная склонность свести информационное противоборство практически исключительно к вопросам пропагандистского обеспечения боевых действий. Поскольку в современном мире информация циркулирует зачастую в реальном масштабе времени, преимущество получает та сторона конфликта, которая обладает наиболее развитой информационной инфраструктурой и способна донести до мирового сообщества информацию о конфликтах под выгодным для себя углом зрения. В качестве удачных действий Джоши приводит информационное освещение индийской армией конфликта в Каргиле, в частности, описывает случай, когда индийская сторона передала тела погибших пакистанских военнослужащих, что сопровождалось широким освещением этого мероприятия в региональных и международных СМИ. По мнению Джоши, подобный шаг позволил решить несколько взаимосвязанных проблем: он укрепил имидж гуманности индийской стороны, наглядно доказал причастность Пакистана к конфликту и в целом склонил международное мнение на сторону Индии. На основании этого делается вывод не только о допустимости, но и полезности проведения подобных информационных операций. Безусловно, при таком подходе невозможно говорить о нарушении международного права, однако вряд ли информационное противоборство будет ограничиваться только такими шагами доброй воли.

Между тем актуальность выработки и подписания договора, ограничивающего информационные виды оружия, вызвана целым рядом причин. Во-первых, широкое применение информационных технологий в военном деле, особенно при обеспечении управления войсками и в системах разведки, способно значительно повысить результативность военных операций при прочих равных параметрах конфликта. Во-вторых, договоры, подобные СНВ или ДОВСЕ, при всех известных издержках обеспечивали соблюдение баланса сил и не позволяли перейти к ситуации с бесконтрольным ростом и развитием вооружений и, как следствие, к актуализации военной конфронтации. В-третьих, независимо от нынешней эффективности систем информационного оружия, появление его в качестве нового фактора противоборства должно учитываться военно-

[17]Joshi Akshay. The Information Revolution and National Power: Political Aspects. Research Officer. *Strategic Analysis*, No.6, Vol.XXIII, September 1999.

политическим руководством, причем невозможность адекватного расчета последствий его применения может привести к асимметричному ответу. В этом случае информационное оружие может послужить катализатором эскалационного развития традиционного конфликта.

При обсуждении проблемы ограничения информационных видов оружия должны рассматриваться не только новые и во многом спорные аспекты информационной войны, такие как ведение сетевой компьютерной борьбы, но и ставшие уже почти традиционными виды боевых действий, которые тем не менее все еще остаются за рамками существующих договоренностей. К таким видам оружия могут быть причислены:

- самолеты-постановщики помех и самолеты дальнего радиолокационного обнаружения, повышающие устойчивость и эффективность боевого управления в ходе войны;
- орбитальные группировки, используемые для сбора и ретрансляции информации в военных целях;
- средства борьбы против энергетических или информационных коммуникаций. Примером такого оружия могут служить так называемые «графитовые бомбы», в целом относящиеся к категории «нелетального оружия», но не обладающие избирательностью действия.

Подводя промежуточный итог обсуждения перспектив переговорного процесса, призванного ограничить возможности ведения информационной войны, можно констатировать, что вопросы регулирования информационного противоборства в полной мере не подпадают под действие ни одного из существующих на сегодняшний день международных соглашений. Более того, в договорах, так или иначе касающихся этих проблем, вопросы информационной безопасности могут трактоваться различными странами не однозначно. Модернизация уже существующих договоренностей с учетом возможности создания информационных систем вооружений, а также высокой уязвимости информационных инфраструктур большинства развитых государств, хотя и представляется желательной, но едва ли осуществима на практике. Это обстоятельство требует инициирования переговорного процесса по заключению принципиально нового соглашения, вводящего однозначно толкуемые требования международно-правовой регламентации различных аспектов ведения информационной войны и информационных операций.

Проблемы контроля и ограничения информационных видов оружия

Контроль над вооружениями, их ограничение и сокращение являются важнейшими задачами обеспечения региональной и глобальной стабильности, удерживающей страны от начала прямой вооруженной конфронтации. Естественно, что решение этих задач всегда является своего рода компромиссом, в котором страны, поступаясь какими-либо своими преимуществами, приобретают определенные гарантии в другой области. В особой мере это касается информационных видов оружия, четкое определение которых пока не выработано, а последствия применения не могут быть адекватно оценены. Однако нынешнее положение не может быть продолжительным, и если в ближайшее время не удастся выработать хотя бы концептуальные основы международных соглашений, ограничивающих новые виды вооружений, это может привести к существенной дестабилизации военно-политической ситуации.

Традиционно задачи, связанные с ограничением каких-либо видов вооружения, рассматриваются в аспектах контроля над вооружениями и режима нераспространения (экспортного контроля).

Контроль над информационными видами вооружений

Частично вопрос контроля над информационными видами оружия уже затрагивался, однако важность проблемы требует более подробного, самостоятельного ее рассмотрения.

На сегодняшний день подписаны и действует несколько важных международных и двусторонних договоров, ограничивающих вооружения и лежащих в основе обеспечения региональной и глобальной стабильности.

Следует признать, что все соглашения вырабатывались и принимались в то время, когда проблема ведения информационных войн еще не стояла столь остро, как сейчас, и за их скобками остались многие аспекты ограничения критических видов вооружений, к которым можно отнести и информационные. Вместе с тем в настоящее время практически все страны, включая США, Россию, КНР и европейские страны, начинают уделять повышенное внимание проблеме ограничения информационных видов оружия. Однако наряду с общим стремлением к выработке взаимоприемлемых договоренностей, способных определить новый баланс сил с учетом информационных возможностей, между этими

странами существуют значительные противоречия в подходах к организации этого процесса. В частности, сама предметная область информационного оружия определена еще очень нечетко, поэтому «правила игры» будут в значительной мере определяться инициаторами (и наиболее активными участниками) переговорного процесса. Так, корпорация РЭНД предлагает Вашингтону воспользоваться настоящим моментом неопределенности для выработки собственных подходов к контролю над вооружениями, экспортному режиму и международной кооперации в области информационных видов оружия, чтобы обеспечить в максимальной степени свою национальную безопасность в будущем[18].

Было бы неправильным полагать, что принципы, выработанные для ограничения ядерного, биологического или химического оружия, могут быть автоматически перенесены на сферу информационного противоборства. Основные различия между традиционными стратегическими вооружениями и информационным оружием заключаются прежде всего в том, что последнее служит целям видоизмененной борьбы на коммуникациях, своего рода «крейсерской борьбы», в то время как традиционные стратегические вооружения направлены против собственно государственной инфраструктуры и живой силы противника. Такие различия уже неоднократно приводили в истории к возникновению дисбаланса сил, при котором одна из сторон была вынуждена выходить за рамки существующих договоренностей, а это ставило под вопрос всю систему стабильности.

Позиция США сводится к стремлению поставить вне закона системы вооружений, направленные против информационных инфраструктур (что для них особенно актуально, т.к. они обладают наиболее развитой и, соответственно, потенциально уязвимой информационной инфраструктурой), и оставить в стороне использование информационных возможностей в традиционной военной сфере.

Другим возможным предметом переговоров, с точки зрения американских экспертов, могут стать те перспективные виды вооружения, в которых на сегодняшний день ни одна из сторон не имеет преимущества. К таковым они относят, например электронно-импульсные системы, предназначенные для атак на информационные системы (т.е., по сути дела, опять компоненты «наступательных» вооружений). Справедливости ради следует отметить, что американские аналитики все больше задаются

[18]Davis Lynn E. Arms Control, Export Regimes, and Multilateral Cooperation. In: The Changing Role of Information in Warfare. RAND, 1999.

вопросом, насколько продолжительным окажется период нынешнего доминирования США и какова должна быть долгосрочная стратегия США в области информационной безопасности[19]. Таким образом, в вопросах обсуждения контроля над информационными вооружениями следует ожидать, что США займут выжидательную позицию.

Режим нераспространения

Задача режима нераспространения или экспортного контроля является двоякой: во-первых, он служит укреплению национальной безопасности государства путем обеспечения и поддержания технологического превосходства; во-вторых, укрепляет общую стабильность, предупреждая, например, использование технологических инноваций в террористических целях.

На западе в годы «холодной войны» для решения первой задачи служил Координационный комитет по многостороннему экспортному контролю (КОКОМ), обеспечивавший лицензирование образцов техники и технологий, запрещенных для поставки в СССР, Китай, Северную Корею и другие коммунистические страны. Решению второй задачи служит ряд межгосударственных договоренностей, таких как соглашение группы ядерных поставщиков, объединяющей около 30 стран, которые установили основные правила контроля за экспортом ядерных материалов, оборудования и технологий. Другим примером подобных договоренностей служит выработанное в 1987 г. соглашение о режиме контроля за ракетной технологией (РКРТ), согласно которому осуществляется контроль за экспортом оборудования и технологий, предназначенных для создания и производства ракет военного или двойного назначения.

Несмотря на достаточно богатый опыт в этой сфере, применение принципов режима экспортного контроля в отношении информационных технологий может вызвать определенные сложности.

Во-первых, под предлогом обеспечения режима нераспространения элементов информационных видов оружия могут ограничиваться возможности ряда стран по свободному использованию международных информационных ресурсов и систем.

[19]По мнению Л. Дэвис, американские военные будут выступать против ограничения любого «нового» типа вооружений до тех пор, пока не будет достигнута адекватная оценка его возможностей и целесообразности.

Во-вторых, ограничение распространения информационных технологий едва ли найдет понимание среди представителей бизнеса, в том числе в высокоразвитых странах. Примером этому может служить положение дел, сложившееся в области распространение технологии использования «длинных» ключей для криптографирования. В качестве аргумента против ограничения их продаж (на чем до 2000 г. настаивали государственные органы США) американские компании выдвигали тезис о том, что аналогичные программы разрабатываются и в других странах, и их распространение на международном рынке, не связанное никакими внутренними препятствиями, постепенно вытеснит американских производителей. Другим примером служит подписанное Президентом США положение, согласно которому к коммерческому использованию допускаются системы GPS с повышенным разрешением (до 10 м), что в принципе достаточно для наведения высокоточного оружия. США пошли на такие меры, поскольку коммерческие выгоды, по их мнению, будут превышать негативные последствия возможного использования данных, полученных с помощью таких систем, другими государствами или отдельными лицами и группами в террористических или военных целях.

В-третьих, международный режим нераспространения должен также учитывать скрытые возможности информационных систем, которые в этой связи должны обязательно проходить процедуру международной сертификации. Об актуальности принятия таких мер свидетельствует череда громких скандалов, связанных с обнаружением «черных ходов» в системах Майкрософт, которые в принципе обеспечивали возможность несанкционированного доступа к информационным ресурсам пользователей.

В связи с этим представляют особый интерес российские инициативы в ООН (подробно будут рассмотрены ниже), в которых предложены принципы международной безопасности в информационной сфере, предусматривающие принятие государствами на себя обязательств воздерживаться от:

- действий, ведущих к доминированию и контролю в информационном пространстве;
- противодействия доступу к новейшим информационным технологиям, создания условий технологической зависимости в сфере информатизации в ущерб другим государствам.

Принятие этих положений, по крайне мере на уровне декларативной политики, позволит избежать использования режима нераспространения,

в целом отвечающего укреплению стабильности, в интересах отдельной страны или группы стран.

Надо отметить, что создание эффективной системы экспортного контроля возможно только на основе многосторонних международных усилий, подкрепляемых созданием международной экспертной комиссии, определяющей возможность использования тех или иных коммерческих систем и технологий в военных целях и оценивающей опасность такого использования для международной стабильности. Кроме того, такая комиссия могла бы решать задачи лицензирования или, по крайней мере, выработки рекомендаций для возможных пользователей относительно обеспечения безопасности работы коммерческих информационных систем.

Международное сотрудничество и кооперация в сфере информационной безопасности

Помимо контроля над вооружениями и экспортного режима существует еще одна область политической активности, в которой могут быть в равной мере заинтересованы все члены международного сообщества. Этой областью является расширение международного сотрудничества и кооперации в сфере информационной безопасности.

Главные задачи такого сотрудничества состоят в решении актуальных проблем, касающихся кризисного управления и планирования, информационных обменов, расширения связей между государствами, а также между их отдельными министерствами и ведомствами с целью гармонизации национальных законодательств и выработки общих усилий по борьбе с терроризмом.

Характерной особенностью стратегии международной кооперации в настоящее время является то, что шаги по ее укреплению не обязательно предпринимаются на глобальном уровне. Вполне допустимо и даже желательно заключение двусторонних или многосторонних договоренностей по мерам обеспечения взаимной безопасности. Впоследствии такие двусторонние и региональные договоренности могут выступать в качестве эталона для выработки соглашений на более высоком уровне и с более широким составом участников. Отсюда следует также, что сторона-инициатор заключения международных договоренностей может приобрести существенные преимущества.

Базовыми элементами для развития такого сотрудничества могли бы стать:

- определение характеристик возникающих угроз, связанных с информационными войнами, и достижение общего понимания потенциальных угроз;
- выработка защитных механизмов и практических методов снижения уязвимости информационных систем и сетей;
- обмен на постоянной основе результатами анализа сложившейся ситуации и информацией о потенциальных противниках и чрезвычайных происшествиях, связанных с работоспособностью информационных инфраструктур, с целью выработки адекватных мер противодействия потенциальным угрозам;
- меры по обнаружению атак на критические информационные инфраструктуры и, в случае их обнаружения, применение той или иной формы принуждения для прекращения атаки;
- меры взаимопомощи в случае повреждений объектов информационных инфраструктур в результате стихийных бедствий.

Естественно, что каждая страна сама должна вырабатывать шаги для снижения собственных специфических рисков, однако приведенные выше положения представляют достаточно хорошую почву для выработки дальнейших международных мер.

Российские инициативы по международной информационной безопасности на международном уровне

Россия еще в середине 1998 г. предложила США подписать на уровне президентов совместное заявление, посвященное исключительно проблематике международной информационной безопасности. Проект документа предлагал видение современной ситуации в информационной сфере, характеризующейся, с одной стороны, качественно новым потенциалом развития человечества, который создает глобальный информационно-технологический прогресс, а с другой — очевидными угрозами использования таких новых технологий в целях, противоречащих общей стабильности и безопасности. Подчеркивалось, что наличие таких угроз требует принятия превентивных мер. Такой процесс мог бы, как предполагалось, предусматривать следующие этапы и меры:

- определение общих взглядов мирового сообщества на проблемы возможного использования информационных технологий в военных целях в качестве оружия;
- определение основных понятий («информационное оружие», «информационная война»);

- учет фактора возможного использования информационных технологий для совершенствования существующих и создания новых систем оружия;
- рассмотрение вопроса о целесообразности создания международной системы (центра) мониторинга угроз, связанных с информационной безопасностью;
- внесение вопроса о глобальной информационной безопасности на рассмотрение ООН и других ведущих международных форумов с целью разработки международно-правового режима запрещения разработки, производства и применения особо опасных видов информационного оружия;
- разработка международного многостороннего договора о борьбе с информационным терроризмом и криминалом.

По мнению российской стороны, такое совместное заявление могло бы способствовать началу конкретного, всестороннего и целенаправленного обсуждения возникающих проблем.

В итоге обсуждения этого предложения идея конкретного заявления по проблемам международной информационной безопасности реализована не была. Однако в общей форме обеспокоенность возникающими угрозам в этой сфере нашла отражение в Совместном заявлении об общих вызовах безопасности на рубеже XXI века подписанного в итоге саммита Президентами России и США 2 сентября 1998 г. в Москве.

В Заявлении, в частности, было отмечено, что стороны:
- «согласились активизировать совместные усилия по противодействию транснациональным угрозам экономике и безопасности наших стран, включая те из них, которые являют собой [...] преступления с использованием компьютерной техники — и других высоких технологий»;
- признали «важность содействия положительным сторонам и ослабление действия отрицательных сторон происходящей информационно-технологической революции, что является серьезной задачей в деле обеспечения стратегических интересов безопасности наших двух стран в будущем»;
- заявили, что «общие вызовы безопасности на рубеже XXI века могут быть отражены только посредством мобилизации усилий всего международного сообщества [...] в случае необходимости мировое сообщество должно своевременно принимать эффективные меры по противодействию таким угрозам».

Таким образом, в общем контексте развития идеи международной информационной безопасности, значение Заявления определяется тем, что в нем впервые две великие державы признали наличие проблемы, обозначили в этой сфере реальные угрозы стратегического характера и были едины во мнении о необходимости комплексного, многостороннего подхода в противодействии этим общим вызовам безопасности. Характерно, что такое взаимное понимание было отражено именно в политическом двустороннем документе.

Дальнейшее развитие тема международной информационной безопасности получила в рамках ООН. 23 сентября 1998 г. Генеральному секретарю ООН К. Аннану было направлено специальное послание Министра иностранных дел России И.С. Иванова[20].

ГА ООН уже на протяжение целого ряда лет рассматривала на своих сессиях вопрос «Роль науки и техники в контексте международной безопасности, разоружения и других, связанных с этим областей». По мнению России, именно такая новая область возникает в связи с качественно новым этапом научно-технического развития — беспрецедентным уровнем развития и внедрения современных, принципиально новых информационных технологий и средств телекоммуникаций.

В послании констатировалось, что информационная революция проникает практически во все сферы жизнедеятельности общества, открывает перспективы для ускоренного развития всей мировой цивилизации и способствует увеличению созидательного потенциала человечества. Формируется глобальное информационное пространство, в котором информация приобретает свойства ценнейшего элемента как национального, так и общечеловеческого достояния, его стратегического ресурса.

При этом, однако, была подчеркнута возможно потенциальная, но от этого не менее серьезная опасность использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности и безопасности, соблюдением принципов неприменения силы, невмешательства во внутренние дела, увеличения прав и свобод человека.

Особый акцент в послании был сделан на необходимости предотвращения появления принципиально новой — информационной —

[20]Распространено в качестве официального документа 53-й сессии ГА ООН (A/C.1/53/3).

области конфронтации, способной спровоцировать новый виток гонки вооружений.

В этой связи подчеркивалось, что речь идет о создании информационного оружия и опасности возникновения информационной войны. Принимая при этом во внимание уровень информатизации общества и одновременно уязвимость информационных структур нельзя исключить возможности появления такого информационного оружия, разрушительные свойства которого могут оказаться сравнимыми с ОМУ.

К посланию был приложен проект резолюции ГА ООН, озаглавленный «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». По сути дела, проект явился развитием упомянутой резолюции ГА о роли науки и техники применительно к конкретной области. В новом проекте, в частности отмечалось, что научно-технические достижения могут иметь как гражданское, так и военное применение и что необходимо поддерживать развитие науки и техники в гражданских целях. Кроме того, в этом документе нашли отражение основные тезисы послания российского Министра иностранных дел. Отмечалась также необходимость предотвращения появления информационных технологий и средств, применение которых в военных целях может оказаться сравнимым с применением ОМУ. В проекте, в частности, содержалось приглашение государствам-членам ООН информировать Генерального секретаря о своей точке зрения и оценках по следующим вопросам:

- общий взгляд на проблемы использования информационных технологий в военных целях;
- определение понятий «информационное оружие», «информационная война», другое враждебное или несанкционированное воздействие на информационно-коммуникационные системы и информационные ресурсы;
- целесообразность разработки международно-правовых режимов запрещения разработки, производства и применения особо опасных видов информационного орудия, а также борьбы с информационным терроризмом и криминалом, включая создание международной системы (центра) мониторинга угроз, связанных с безопасностью глобальных информационно-коммуникационных систем.

Инициативные предложения России вызвали активное обсуждение в Первом комитете, в результате которого проект резолюции был модифицирован в основном в части рекомендаций относительно информирования Генерального секретаря о точках зрения и оценках

государств-членов. 2 ноября 1998 г. пересмотренный проект был одобрен Комитетом, а 4 декабря 1998 г. принят без голосования (консенсусом) ГА ООН (документ A/RES/53/70)[21].

В части упомянутых рекомендаций резолюция предусматривала информировать Генерального секретаря по следующим позициям:

- общая оценка проблем информационной безопасности;
- определение основных понятий, относящихся к информационной безопасности. Включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов;
- целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали борьбе с информационным терроризмом и криминалом.

Таким образом, прямые ссылки первоначального российского проекта на использование информационных технологий в военных целях, определение конкретных понятий «информационное оружие» и «информационная война», разработки режима запрещения разработки и применения информационного оружия, а также положений о сравнении воздействия информационного оружия и ОМУ в принятой резолюции отражения не получали.

В заявлении делегации США по мотивам голосования в Первом комитете ГА ООН (вопросы разоружения и международной безопасности) отмечалась «гибкость, продемонстрированная основным спонсором резолюции в продвижение этой инициативы». По мнению американской стороны, одобренный текст отражает сбалансированный подход, который позволит международному сообществу начать тщательное, обдуманное рассмотрение этой новой и сложной темы. В то же время, было подчеркнуто, что одобрение резолюции означает вступление международного сообщества в процесс решения задач, включающих многие взаимосвязанные факторы, не относящиеся обычно к компетенции Первого комитета. Эта тема включает, например, технические аспекты, связанные с экономическим сотрудничеством и торговлей, интеллектуальной собственностью, правоохранительной деятельностью, борьбой с терроризмом и другими вопросами, рассматриваемыми во Втором (экономические и финансовые вопросы) и

[21]Текст этой и последующих резолюций, принятых по вопросам информационной безопасности, а также связанные с ними доклады Генерального секретаря ООН, приведены в Приложении 4.

Шестом (правовые вопросы) комитетах ГА. Кроме того, не следует фокусироваться исключительно на действиях правительств и их программах, поскольку данная инициатива также затрагивает существенные интересы личностей, предприятий и других организаций в частном секторе.

Резолюция постановила включить тему международной информационной безопасности в повестку дня очередной 54-й сессии ГА ООН.

В последующий период в соответствии с рекомендациями пунктов 2 и 3, резолюции 53/70 Генеральному секретарю ООН были представлены соответствующие оценки правительств (Австралия, Белоруссия, Бруней, Куба, Оман, Катар, Российская Федерация, Великобритания и США), опубликованные в докладе A/54/213.

Мнение *Австралии* сводилось к тому, что, несмотря на актуальность проблемы, эта страна не разделяет мнения о том, что подходящим органом для разработки принципов обеспечения безопасности глобальных информационных систем является Департамент по вопросам разоружения Секретариата ООН. Информационная инфраструктура действительно оказывает влияние на торговлю, экономику, общественное благосостояние планеты, правопорядка и безопасности. Но принципы и руководящие указания по этим вопросам уже разработаны на других форумах (Организация экономического сотрудничества и развития, Международная организация по стандартизации, Международный союз электросвязи, международные центры по предупреждению преступности), причем с применением более широких подходов, чем это предложено в резолюции 53/70. Австралия не видит смысла в дублировании такой работы.

В мнении *Белоруссии* отмечалось своевременность принятия резолюции и поддерживалась идея о разработке концепции международной информационной безопасности и принципов, направленных на укрепление безопасности глобальных информационных систем и предупреждение информационного терроризма и преступности.

Бруней, признавая важность информационной безопасности в эпоху информационных технологий, считал, однако, что ответственность за обеспечение гарантий безопасности международных коммуникаций не следует относить к выходящим за рамка компетенции Международного Суда ООН.

В оценках *Кубы*, в частности, отмечалось, что процесс «компьютеризации общества», вступление в «информационный век» создает новые проблемы безопасности, требующие рассмотрения всем международным сообществом. ООН является подходящим форумом для обсуждения этих проблем. Кроме того, должны приниматься меры для обеспечения доступа к новым информационным технологиям в целях развития, особенно слаборазвитых стран. Следствием процесса глобализации в сфере информатизации и телекоммуникаций является широкая стандартизация в сфере информационных технологий, облегчающая вмешательство в такие системы. Куба считает, что информационные технологии, создаваемые в развитых странах и их доминирующее положение позволит навязывать технологические стандарты, облегчающие использование таких технологий, как средство агрессии.

Считается, что у слаборазвитых стран нет другой альтернативы, как принять эти технологии, чтобы выжить в новых условиях. Во многих случаях эти страны не осознают возникающие угрозы и не принимают мер обеспечения безопасности.

Серьезные последствия имеет развитие и глобальных сетей типа интернет, функционирующих на чисто кооперативной основе. Такая добровольная основа интернет является одновременно источником его сильных и слабых качеств, поскольку страны не приняли единообразного законодательства, в отношении подобных сетей.

Куба полагала, что безопасности информации включает защиту ее конфиденциальности (доступность только тем, кто имеет право на ее использование), защиту информации от несанкционированного изменения (неприкосновенность), а с другой стороны — защиту от отказа в обслуживании (общая доступность).

В этой связи в оценках Кубы приводится ряд критериев, которые можно свести к следующим:

- пользователи должны нести ответственность за собственное поведение, т.е. несанкционированный доступ к информационным ресурсам является нарушением, независимо от того, насколько защищены такие ресурсы;
- организации, пользующиеся информационными технологиями, несут ответственность за их надлежащее использование своими сотрудниками;
- поставщики услуг несут ответственность за обеспечение безопасности своих систем;

- пользователи и поставщики услуг должны сотрудничать в обеспечении информационной безопасности.

Что касается межгосударственных отношений, то использование информационных систем и ресурсов для вмешательства в дела других стран является нарушением суверенитета и создает очаги напряженности, представляющие серьезную угрозу международной безопасности.

По мнению Кубы, развитие информационных технологий несомненно требует параллельного развития международного права в этой области. Эта непростая задача может быть облегчена с учетом уже принятых принципов и международно-правовых документов в области науки и техники.

В качестве таких источников Куба указывала следующие:
- резолюция ГА ООН 110 (II) от 3 ноября 1947 г., в которой осуждается пропаганда, имеющая целью создать или усилить угрозу миру, нарушение мира или акт агрессии;
- международно-правовые документы ЮНЕСКО и Международного союза электросвязи;
- принципы использования государствами ИСЗ для непосредственного телевизионного вещания, принятые ГА ООН;
- положения о защите конфиденциальной информации в приложении к Конвенции о запрещении химического оружия.

По мнению Кубы, международное сообщество должно признать тот факт, что каждая страна имеет право на защиту своих информационных ресурсов. В рамках ООН могут быть заключены многосторонние договоры, запрещающие агрессивные действия в отношении таких ресурсов. Можно было бы также рассмотреть идею соглашений, гарантирующих использование разрабатываемых информационных технологий в мирных целях и их доступность для всех государств.

В качестве наиболее характерных моментов в информации *Омана*, видимо, можно отметить право государственного органа по телекоммуникациям этой страны ограничивать доступ к информации в общественной сфере через определенные каналы, например интернет. В действующих в стране правилах предусматривается правовая защита информации в части как ее материальной ценности, так и нравственных аспектов.

Оманом поддерживается идея разработки международных принципов, направленных на укрепление безопасности информационных систем.

По мнению *Катара*, общей оценке проблемы информационной безопасности может способствовать обмен техническими знаниями и понимание опасности несанкционированного вмешательства и его воздействия на безопасность и финансовые аспекты. Методами обеспечения информационной безопасности могут быть:

- шифрование;
- применение программ, обеспечивающих контроль доступа к данным;
- проверка права пользователя на доступ к данным;
- применение аппаратных и программных средств сетевой защиты.

Наиболее развернутый документ по данной теме был представлен *Российской Федерацией*. В документе были детализированы общие подходы и оценки Россией проблематики международной информационной безопасности, изложенные ранее в послании Генеральному секретарю ООН. Кроме того, в общих положениях отмечалось, что увеличение за счет новейших информационных технологий военного потенциала отдельных стран ведет к изменению глобального и регионального балансов сил, возникновению напряженности между традиционными и нарождающимися центрами силы и влияния.

Универсальности, скрытность или обезличенность, возможность широкого трансграничного применения, экономичность и общая эффективность делают информационное оружие чрезвычайно опасным средством воздействия, причем разработка и применение такого оружия практически не регулируется нормами современного международного права.

По мнению России, возникает очевидная потребность в международно-правовом регулировании мировых процессов гражданской и военной информатизации, разработке согласованной международной платформы по проблеме международной информационной безопасности. При этом была предложена модель действий международного сообщества, которая предусматривала дальнейшее рассмотрение ситуации в сфере международной информационной безопасности и принятие ГА ООН новых резолюций, конкретизированных в части ограничения угроз как криминального, так и военного характера.

Россия предлагала, по мере определения общих подходов, вести дело к разработке принципов международной информационной безопасности (режима, кодекса поведения государств), которые могли бы быть первоначально сформулированы в виде многосторонней декларации, а в перспективе закреплены в форме международно-правового документа. Проработку этих вопросов предлагалось вести также и в рамках женевской Конференции по разоружению.

При этом предлагалось исходить из необходимости принятия таких принципов в комплексе, т.е. применительно как к военной, так и гражданской сферах.

Далее в оценках России излагалось понимание основных угроз в этой сфере и основных задач и целей разработки режима международной информационной безопасности. Кроме того, были предложены терминологические формулировки основных понятий, относящихся к этой проблематике, включая определения собственно «международной информационной безопасности», а также «информационной войны» и «информационного оружия».

Все эти основные подходы, понимание угроз, задач международного сообщества и использование терминов впоследствии составили основу предложенного Россией проекта документа «Принципы, касающиеся международной информационной безопасности»[22] (см. Приложение 4).

В заключении *Саудовской Аравии* отмечалось, что по мере ускорения прогресса в области информационных технологий одновременно возрастает и число актов, направленных на нарушение функционирования информационных систем, их дестабилизацию и вмешательство в них, которые предпринимаются в преступных целях. Такая деятельность наносит ущерб экономике и подрывает безопасность. Внедрение международных принципов и норм имеет важное значение с тем, чтобы противостоять угрозам информационной безопасности. Соответствующие международные организации должны следить за тем, чтобы виновные в совершении таких актов представали перед правосудием и несли наказание.

По оценке *Великобритании*, связь между информационными системами во всем мире достигла такой степени, что большинство государств подвергается опасности электронного нападения со стороны

[22]Опубликован в докладе Генерального секретаря ООН, документ A/55/140 от 10 июля 2000 г.

преступников и террористов на жизненно важные элементы их инфраструктуры.

По мере расширения использования компьютерных систем, такая опасность будет возрастать. Поскольку эти системы связаны между собой на международном уровне, данная угроза приобретает трансграничный характер и представляет собой проблему для всех членов ООН. Соединенное Королевство приветствует шаги по изучению соответствующих средств борьбы, включая и многостороннюю основу, которые могли бы обеспечить неприкосновенность от подобных нападений.

Правительство Великобритании принимает меры безопасности на своем национальном уровне. Однако, учитывая характер угроз, оно признает важное значение международного сотрудничества в этом вопросе. Соответствующий диалог включает работу Группы «восьмерки» по вопросам преступности в сфере высоких технологий и в Совете Европы (разработка Конвенции о кибернетической преступности).

Соединенное Королевство полагает, что ООН необходимо следить за ходом работы на этих форумах с тем, чтобы учитывать ее в определении собственных мероприятий. В их число могла бы входить разработка международных принципов укрепления безопасности глобальных систем и содействия борьбе с международным терроризмом и преступностью.

Соединенные Штаты Америки рассматривают информационную безопасность как сложную тему, затрагивающую многие факторы и виды деятельности отдельных лиц, групп и правительств. Эта общая тема включает аспекты, связанные с международным миром и безопасностью (работы Первого комитета ГА ООН), но также охватывает технические аспекты глобальных коммуникационных систем, равно как и нетехнические вопросы экономического сотрудничества и торговли, правами интеллектуальной собственности, соблюдением законности, борьбы с терроризмом и др., рассматриваемые во Втором или Шестом комитетах.

Касаясь аспектов, непосредственно затрагивающих международную безопасность, США отметили, что методы использования электромагнитных импульсов для борьбы с противником далеко не новы. В будущем же, для вооруженных сил важное значение будет иметь защита их собственных информационных сетей.

Кроме того, государствам необходимо располагать потенциалом для восстановления информационных сетей в случаях чрезвычайных ситуаций. Информационная безопасность охватывает также защиту данных, связанных с военным потенциалом и другими аспектами национальной безопасности.

Концепция информационной безопасности предполагает защиту результатов научных исследований коммерческого характера, технологий и других видов конфиденциальных данных (планы маркетинга, работа с клиентурой) и связана также с обеспечением выполнения международных договоров об интеллектуальной собственности.

Что касается технических аспектов, то, по мнению США, положения Международного союза электросвязи и меры национальных учреждений обеспечивают надежность международной сети связи. Соответствующие же стандарты обеспечивают гарантии производителям и пользователям электронных устройств.

США рассматривают потенциальную опасность использования преступниками информационных технологий как проблему, представляющую интерес для всех государств и разделяют мнение о необходимости в одностороннем и многостороннем порядке содействовать обеспечению неприкосновенности соответствующих ресурсов.

США также полагают, что любое незаконное вмешательство или попытки нарушить любой аспект их национальных информационных систем представляют угрозу их национальным интересам. Признавая потенциальную серьезность такой угрозы, США инициировали реализацию национальных программ в государственном и частном секторах по защите важных объектов инфраструктуры. В то же время, учитывая глобальную взаимозависимость инфраструктур, усилия на национальном уровне будут в конечном счете зависеть и от степени безопасности систем, находящихся за пределами США.

Поэтому США считают, что всем государствам следует принять на национальном уровне меры с тем, чтобы преступники или террористы, действующие на их территории и нарушающие функционирование информационных систем, карались за это.

Тема информационной безопасности имеет много чрезвычайно переплетенных измерений. Учитывая несомненную необходимость в анализе

всех аспектов этой темы, было бы преждевременным приступать к разработке всеобъемлющих принципов информационной безопасности. Вместо этого международному сообществу следует проделать значительную работу, чтобы на систематической основе осмыслить пройденный этап, прежде чем двигаться дальше. В этих целях государствам необходимо стремиться к ознакомлению с идеями и мнениями широкого круга экспертов.

Тем не менее международное сотрудничество имеет важное значение в деле решения проблем, порождаемых информационным терроризмом и преступностью. Совет Европы изучает проект Конвенции о киберпреступности, Группа «восьмерки» по вопросам преступности в области высоких технологий изучает меры правовой взаимопомощи. Организация азиатских государств также учредила подобную группу, Азиатский и дальневосточный институт ООН по предупреждению преступности и обращению с правонарушителями изучает смежные вопросы.

Все эти усилия заслуживают высокой оценки, и их надо активизировать. Было бы недальновидно, полагают США, если бы ГА ООН занялась разработкой стратегий и мероприятий, способных нанести ущерб уже проводимой работе.

В соответствии с рекомендациями резолюции 53/70 Институтом ООН по проблемам разоружения (ЮНИДИР) и Департаментом по вопросам разоружения Секретариата ООН в августе 1999 г. в Женеве был организован международный семинар по вопросам международной информационной безопасности. В семинаре приняли участие представители более 50 стран, включая экспертов из наиболее развитых в информационно-технологическом плане государств.

Задача семинара заключалась в выявлении подходов различных стран в связи с предстоящим продолжением дискуссии по этой теме на 54-й сессии ГА ООН. Основным итогом семинара стало подтверждение актуальности проблемы информационной безопасности и своевременности постановки этого вопроса в международном плане.

В то же время в рамках обсуждения обозначились по крайней мере два различных подхода к существу проблемы.

Эксперты ряда развитых стран, включая США, исходили из приоритета рассмотрения и разработки мер информационной безопасности применительно к угрозам террористического и криминального характера.

При этом угроза создания информационного оружия и возникновения информационной войны сторонниками такого подхода рассматривалась больше как теоретическая. Соответственно отпадал и собственно разоруженческий аспект общей проблемы международной информационной безопасности. Дальнейшее обсуждение этой проблематики предлагалось рассредоточить по региональным и тематическим форумам (Европейский Союз, «восьмерка», Организация азиатских государств, Организация экономического сотрудничества и развития и т.д.), а в рамках ООН перевести из Первого комитета во Второй (экономические вопросы) и Шестой (правовые вопросы).

С другой стороны, приверженцы иного курса (в основном представители развивающихся стран) поддерживали концепцию рассмотрения проблемы международной информационной безопасности в комплексе, с выделением в качестве приоритетной задачи ограничение потенциальной угрозы развязывания информационной войны. При этом подчеркивалась необходимость безотлагательно приступить к обсуждению и практической разработке международно-правовой основы универсального режима международной информационной безопасности. Выдвигалось, в частности, предложение о создании специального международного суда по преступлениям в информационной сфере.

В любом случае эта первая такого рода представительная встреча экспертов, несомненно, во многом способствовала выполнению рекомендации резолюции 53/70.

1 декабря 1999 г. ГА ООН консенсусом был принят обновленный российский проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (№54/49). В резолюции, в частности, отмечалась своевременная инициатива Секретариата ООН и ЮНИДИР по проведению указанной встречи экспертов в Женеве, способствовавшей лучшему пониманию существа проблем международной информационной безопасности, связанных с ними понятий и возможных мер ограничения возникающих в этой сфере угроз.

Новым моментом в резолюции 54/49, отразившим в том числе и итоги дискуссии на этой женевской встрече, стало указание на то, что «информационные технологии [...] могут негативно воздействовать на безопасность государств применительно как к гражданской, так и военной сферам»[23]. Таким образом, если резолюция 1998 г. лишь

[23]Восьмой абзац преамбулы резолюции 54/49.

обозначила наличие общей проблемы, то последующая недвусмысленно указала на ее военное и, соответственно, разоруженческое измерение. Эта резолюция подтвердила ранее зафиксированные рекомендации и постановила включить тему международной информационной безопасности в повестку дня очередной, 55-й сессии ГА ООН.

55-й сессии ГА ООН был также представлен соответствующий очередной доклад Генерального секретаря ООН[24]. В доклад вошли оценки Иордании, Катара и России.

Суть ответа *Иордании* заключалась в констатации возможностей злоупотребления новейшими достижениями в области информационно-технологических систем и, в частности, их использовании в террористических целях. В качестве мер безопасности в отношении такой деятельности Иордания предложила разработать специальное чрезвычайное законодательство, с тем чтобы, в частности, позволить службам безопасности получать доступ в центры управления компаниями, связанными с этими системами, и частично контролировать их.

Катар представил свои формулировки некоторых определений, связанных с информационной безопасностью.

Российская Федерация предложила проект документа, озаглавленного «Принципы, касающиеся международной информационной безопасности». Формат Принципов соответствует принятой ООН практике и, в частности, целому ряду документов по вопросам космоса, принятых ГА (Декларация принципов деятельности государств по исследованию и использованию космического пространства, Принципы использования искусственных спутников Земли для международного непосредственного телевизионного вещания, Принципы, касающиеся дистанционного зондирования и ряд других). Принятые и одобренные в форме резолюций ГА ООН, эти документы, строго говоря, не являются договорами и тем не менее возлагают на голосовавшие за них государства по крайней мере политические и моральные обязательства по выполнению соответствующих положений.

Практическое значение предлагаемого проекта Принципов международной информационной безопасности и дальнейшего предметного обсуждения проблематики международной информационной

[24]Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Документ A/55/140.

безопасности очевидно, поскольку в этом документе прежде всего предлагается понятийный аппарат — определения таких базовых терминов, как информационное оружие, информационная война и собственно информационная безопасность.

Основная идея документа сформулирована в положениях Принципа I — деятельность каждого государства в информационном пространстве должна способствовать общему прогрессу и не противоречить задаче поддержания мировой стабильности и безопасности, интересам безопасности других государств, принципам неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека.

В связи с этим последним положением относительно прав и свобод человека, характерно закрепление в проекте Принципов идеи о том, что такая деятельность должна быть совместимой с правом каждого искать, получать и распространять информацию. При этом, однако, отмечается, что такое право может быть ограничено законом в целях защиты безопасности каждого государства. Кроме того, все члены международного сообщества должны, в соответствии с Принципами иметь равные права на защиту своих информационных ресурсов и критически важных структур от несанкционированного информационного вмешательства.

Принципы также дают определения основных угроз в сфере международной информационной безопасности и формулируют направления деятельности, которые могли бы способствовать созданию международно-правовой основы ограничения таких угроз.

Вынесение темы «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» на повестку дня очередной, 55-й сессии ГА ООН вновь подтвердило заинтересованность международного сообщества в обсуждении этой актуальной проблематики. Принятая в итоге, опять-таки консенсусом, резолюция 55/28 подтвердила ранее принятые рекомендации. Резолюция призывает государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также рассмотрению возможных мер по ограничению угроз, возникающих в этой сфере.

Новым моментом в резолюции стало положение (пункт 2) о том, что целям таких мер соответствовало бы изучение соответствующих международных концепций, которые были бы направлены на укрепление

безопасности глобальных информационных и телекоммуникационных систем.

Призывая государства-члены и далее информировать Генерального секретаря ООН о своих оценках по проблематике международной информационной безопасности, резолюция прямо указывает в этой связи (пункт 3c) на содержание концепций, упомянутых в пункте 2.

Сдержанность в отношении активной поддержки дальнейшего развития идеи международной информационной безопасности большинство западных стран объясняют сложностью, новизной рассматриваемой проблематики, а также опасениями возможных ограничений свободы обмена информацией и конкуренции на рынке информационных технологий, которые якобы могут возникнуть в случае реализации этой идеи.

По мнению ряда западных экспертов, массированные информационные атаки могут быть осуществлены с помощью обычных персональных компьютеров с использованием широких технологических возможностей, доступ к которым предоставляет интернет. Причем правительства при этом якобы не участвуют ни в разработке, ни в контроле за подобными технологиями. Иначе говоря, на сегодня международное сообщество не обладает ни техническими возможностями, ни правовым инструментом, чтобы достаточно точно идентифицировать инициатора такой атаки и, соответственно, «наказать» его. Кроме того, атаки могут фактически осуществляться государствами, но, что называется, «чужими руками» (что позже — в апреле-мае 2000 года — подтвердилось в хакерской войне США-КНР). И, напротив, какая-либо третья сторона может провести информационное нападение таким образом, что его инициатором будет выглядеть невиновное государство (как это, например, было при нападении на Индонезию с территории европейских стран). Соответственно, утверждают они, надежные, конкретные и практически применимые ограничения таких угроз создать и реализовать в настоящее время на практике невозможно. Примечательно, что выдвинув свою резолюцию 55/63 по киберпреступности они фактически провозгласили обратное.

При этом считается, что нормы международного права, действующие в отношении вооруженных конфликтов и, в частности, принципы военной необходимости, пропорциональности и ограничения косвенного ущерба уже регулируют использование информационных технологий в ходе таких конфликтов. Т.е. в разработке каких-либо новых международных принципов необходимости якобы нет. Кроме того, утверждается, что, если

какие-то государства и возьмут на себя обязательства следовать определенному кодексу поведения, это не ограничит наиболее вероятных угроз информационной безопасности террористического или иного преступного характера. Ведь преступники, мол, по определению не собираются следовать условиям международных договоренностей.

Все эти мнения, очевидно, могут и должны быть приняты во внимание, но, видимо, не более чем дополнительные основания к необходимости решения проблемы международной информационной безопасности именно в международно-правовом плане.

Действительно, многие «традиционные» действия, уже применяемые в ходе военных конфликтов (прямое боевое воздействие на информационные структуры противника, подавление радиосигналов и т.п.), могут рассматриваться в рамках действующих международных норм, поскольку при этом применяется традиционное оружие и военная техника, а целью применения является физическое уничтожение таких систем. Сегодня, однако, кажется, что победа, достигнутая за счет полного разрушения инфраструктуры противника, теряет смысл. В этой связи, принципиальное отличие информационного оружия и заключается в том, что ущерб от его использования в отношении критических структур не обязательно связан с физическим разрушением их компонентов. И тем не менее в конкретных случаях такой ущерб, учитывая жизненно важный характер этих структур, может иметь катастрофические последствия, сравнимые по своим последствиям с результатами применения ОМУ.

Действительно, на первый взгляд несанкционированное воздействие (вмешательство) в информационную систему, данные которой не засекречены, вряд ли можно квалифицировать как применение оружия. Рассмотрим, однако, некоторые, возможно гипотетические примеры. В результате скоординированной атаки на компьютерные сети отключается система контроля воздушного движения, что, в свою очередь, вызывает катастрофу самолета с человеческими жертвами. Или включен несанкционированно сброс воды в крупном водохранилище, результат — наводнение, разрушения в инфраструктуре и вновь человеческие жертвы. Даже, возможно, и не вызывая жертв, такие вмешательства в компьютеризированные системы управления критических структур государства (электроснабжения, оборонного и военно-промышленного секторов, правоохранительных органов и т.п.) могут вызывать прямые угрозы национальной безопасности.

В этой связи можно сделать очевидный вывод, что современные информационные технологии могут использоваться в качестве оружия. Причем воздействие такого оружия качественно отличается от традиционного, и, соответственно, вопросы его дальнейшего развития, распространения и возможного применения должны стать предметом специальных норм международного права. Вся история развития новых видов оружия начиная от обычного и кончая ракетно-ядерным говорит о том, что международное сообщество в итоге находило разработку таких норм рациональной и необходимой. Проблема, однако, в том, что эти меры разрабатывались чаще всего уже после того, как новое оружие было изобретено и применено.

Кроме того, по многим признакам международное информационное пространство можно рассматривать в качестве общего наследия человечества. Интернет, в частности, используется всеми государствами и конкретно не должен принадлежать никому. Очевидно, что этот тезис подтверждает необходимость применения в этом пространстве особого международного режима, регулирующего деятельность в нем каждого с учетом интересов всех. Сложность разработки такого режима очевидна, поскольку международное сообщество сталкивается здесь с задачей кодификации не только весьма новой и сложной с технической точки зрения области деятельности, но, и это, видимо, главное, — крайне чувствительной для их безопасности сферы.

На определенные исторические параллели в подходах можно сослаться применительно к развитию морского права (успешная разработка исключительно сложной Конвенции по морскому праву 1982 г.) и космического права. Особенно характерен прогресс в кодификации космической деятельности.

Начавшаяся с запуском в 1957 г. первого спутника научно-техническая революция в использовании космического пространства мгновенно выдвинула целый ряд сложных вопросов как правового характера, так и связанных с международной безопасностью политических проблем. При этом характерно, что разработка правовой базы шла поэтапно — один договор опирался на другой, причем параллельно решались общие принципы деятельности в космосе (Договор о космосе 1967 г.) и проблемы ограничения конкретных действий государств в этой сфере, представляющих угрозу мировой безопасности и стабильности (Договор о запрещении ядерных испытаний в атмосфере, космосе и под водой 1963 г., Договор об ограничении систем ПРО 1972 г.).

Для регулирования же тех направлений деятельности, которые по различным причинам «не укладывались» в рамки строго обязательных договорных документов, также были найдены приемлемые формы деклараций и принципов, одобренных всеми или большинством стран-членов ООН.

Очевидно, что если международное сообщество сможет найти общее понимание подходов, изложенных в российском проекте Принципов международной информационной безопасности, этот документ можно было бы рассматривать в качестве «концепции» упомянутой в резолюции 55/28 и использовать в дальнейшем как основу многостороннего договора (конвенции), создающего универсальный режим международной информационной безопасности.

При этом основной идеей такого договора могло бы стать обязательство участников не прибегать к действиям в информационном пространстве, целью которых является нанесение ущерба информационным системам, процессам и ресурсам другого государства, его критически важным структурам, подрыв политической, экономической и социальной систем, массированная психологическая обработка населения с целью дестабилизации общества и государства.

С этой целью и в духе создания режима коллективной информационной безопасности участники договора также откажутся от:

- разработки, создания и использования средств воздействия и нанесения ущерба информационным ресурсам и системам другого государства;
- несанкционированного вмешательства в информационно-телекоммуникационные системы и информационные ресурсы, а также их неправомерного использования;
- действий, ведущих к доминированию и контролю в информационном пространстве;
- противодействия доступу к новейшим информационным технологиям, создания условий технологической зависимости в сфере информатизации в ущерб другим государствам;
- поощрения действий международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющих угрозу информационным ресурсам и критически важным структурам государств;
- разработки и принятия планов, доктрин, предусматривающих возможность ведения информационных войн и способных

спровоцировать гонку вооружений, а также вызвать напряженность в отношениях между государствами и собственно возникновение информационной войны;
- использования информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере;
- трансграничного распространения информации, противоречащей принципам и нормам международного права, а также внутреннему законодательству конкретных стран;
- манипулирования информационными потоками, дезинформации и сокрытия информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этических и эстетических ценностей;
- информационной экспансии, приобретения контроля над национальными информационно-телекоммуникационными инфраструктурами другого государства, включая условия их функционирования в международном информационном пространстве.

В этом случае такой договор должен содержать:
- определения признаков и классификации информационной войны, информационного оружия и средств, которые можно отнести к информационному оружию;
- меры по ограничению оборота информационного оружия;
- режим запрещения разработки, распространения и применения информационного оружия;
- меры предотвращения угрозы возникновения информационной войны;
- положение о признании опасности применения информационного оружия в отношении критически важных структур, сравнимой с опасностью применения ОМУ;
- условия для равноправного и безопасного международного информационного обмена на основе общепризнанных норм и принципов международного права;
- меры предотвращения использования информационных технологий и средств в террористических и других преступных целях;
- разработку процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия;
- условия создания системы международного мониторинга для отслеживания угроз, проявляющихся в информационной сфере и механизма контроля выполнения условий режима международной информационной безопасности;

- механизм разрешения конфликтных ситуаций в сфере информационной безопасности;
- условия создания международной системы сертификации технологий и средств информатизации и телекоммуникации (в том числе программно-технических) в части гарантий их информационной безопасности;
- мирное развитие системы международного взаимодействия правоохранительных органов по предотвращению и пресечению правонарушений в информационном пространстве;
- рекомендации по гармонизации на основе добровольности национального законодательства в части обеспечения информационной безопасности.

В соответствии с договором государства и другие субъекты международного права должны будут нести международную ответственность за деятельность в информационном пространстве, осуществляемую ими, под их юрисдикцией или в рамках международных организаций, членами которой они являются, и за соответствие любой такой деятельности положениям договора.

Конечной целью усилий мирового сообщества, и на это направлены российские инициативы, должно стать провозглашение информационного пространства зоной, свободной от оружия.

ЗАКЛЮЧЕНИЕ

Россия даже при значительном ослаблении своей экономической и военной мощи остается влиятельным центром силы. Положение России в мире определяется прежде всего факторами внутреннего развития, которые в свою очередь существенно зависят от характера отношений с государствами СНГ, соседними странами Европы и Азии и США.

Территория России — это естественный мост между Европой и Азиатско-Тихоокеанским регионом. Ее размеры и огромные естественные ресурсы таят в себе громадные возможности будущего развития. В годы глобального противостояния, когда мир был разделен идеологическими и экономическими барьерами, территория России не могла стать регионом, объединяющим два мировых экономических центра. Сегодня это должно стать одной из наиболее важных геополитических целей России в XXI веке.

Каким же видится адекватный ответ России на появление информационного оружия и угрозы информационной войны? Очевидно, что ответ на этот вопрос может быть дан только в контексте общей политики государства в области обеспечения национальной безопасности.

Прежде всего надо трезво осознать, что Россия потеряла свои прежние стратегические позиции великой военной державы и выработка новой реальной политики обеспечения национальной безопасности, отвечающей ее интересам и весьма ограниченным возможностям, является актуальной и приоритетной задачей. По нашему мнению, в основу этой политики должно быть положено понимание долгосрочных целей и приоритетов развития страны, а не амбиции великодержавности, как реликты политического мышления[1]. Сегодня стереотипы конфронтационного мышления, принципы и методы поддержания стратегической стабильности и обеспечения национальной безопасности, выработанные во времена глобального противостояния двух великих держав, являются препятствием для формирования рациональной политики, учитывающей новые реалии и отвечающей национальным интересам России.

Россия стремится быть равноправным членом сообщества демократических развитых стран мира, занимать свою нишу в мировом

[1] Нужно помнить, что положившая начало «холодной войне» фултоновская речь У. Черчилля была произнесена в период, когда СССР был на пике своей политической и военной силы.

разделении труда, быть мостом между Европой и Азиатско-Тихоокеанским регионом. В военно-политическом плане она должна остаться силой, обеспечивающей стабильность на громадном евроазиатском пространстве. Для достижения этих долгосрочных национальных целей наиболее благоприятным направлением ее военной политики было бы развитие стратегического сотрудничества со странами Европы, США, Китаем и другими государствами в совместной борьбе с современными и будущими вызовами безопасности.

Сегодня вопросы национальной безопасности все более пересекаются с проблемой глобальной безопасности и, следовательно, должны будут во многом решаться в рамках партнерства и сотрудничества. Наиболее важной областью такого сотрудничества является обеспечение национальной и международной информационной безопасности.

Для выработки рациональной политики в области обеспечения информационной безопасности прежде всего необходима трезвая оценка сегодняшнего состояния, особенностей и перспектив развития информационного оружия и способов его применения. Такая оценка есть базовая предпосылка выработки внешней и внутренней политики государства, военные и военно-технические компоненты которой могли бы предотвращать или парировать возникшие угрозы и надежно обеспечивали бы безопасность страны.

При этом важно понять, что угроза информационной войны и информационной преступности в широком контексте есть фактор скрытого военно-политического давления и запугивания, фактор, способный нарушить мировую и региональную стабильность и безопасность. Именно поэтому в широком плане должен осуществляться мониторинг угроз применения информационного оружия и перманентная оценка эффективности функционирования систем противодействия этому оружию. Такой мониторинг должен охватывать не только научно-технические и технологические достижения в разработках информационного оружия и средств противодействия ему, но и динамику предпосылок и условий его возможного применения, т.е. изменения внешнеполитической ситуации, прогноз глобальных и локальных противоречий и конфликтов, несущих с собой угрозу информационной войны.

Естественным было бы отслеживать также состояние внутреннего и международного законодательного и нормативно-правового обеспечения информационной безопасности.

Естественной реакцией на появление нового высокотехнологичного оружия является создание адекватных средств противодействия. Речь должна идти не только о технологиях обнаружения воздействий информационного оружия, но и о своего рода «системах раннего предупреждения» о его вероятных применениях. Эти средства должны дополняться методами контруправления информационным оружием, а также разнообразными правовыми и организационно-экономическими мерами, направленными на защиту государственных информационных ресурсов.

Экономическую и научно-техническую политику государства следует также рассматривать через призму информационной безопасности. Будучи открытой, ориентированной на соблюдение законных прав граждан на информацию и интеллектуальную собственность, эта политика должна быть протекционистской, поддерживающей отечественных производителей технологий, защищающих внутренний рынок от проникновения в него скрытых элементов информационного оружия. Это особенно важно сегодня, когда основная масса информационных технологий поступает из-за рубежа.

В эпоху глобализации информационных систем без подключения к мировому информационному пространству любую страну ожидает экономическое прозябание. Однако следует отчетливо представлять себе, что участие России в международных системах телекоммуникаций и информационного обмена невозможно без комплексного решения проблем информационной безопасности.

Следовательно, необходимо международное сотрудничество, ориентированное на разработку и принятие правовых положений и соглашений, обеспечивающих информационную безопасность в процессах трансграничного информационного обмена. Необходима активная поддержка деятельности различных международных групп, разрабатывающих и обсуждающих различные аспекты внутреннего и межгосударственного законодательства, международные стандарты и возможные области взаимных интересов стран в информационной сфере. В частности, должны быть определены и юридически закреплены меры международного характера, направленные на предотвращение и обеспечение ответственности за компьютерные преступления.

Ясно, что запретить разработку и использование информационного оружия на нынешнем этапе вряд ли удастся, как это сделано, например,

для химического или бактериологического оружия. Понятно также, что ограничить усилия многих стран по формированию единого глобального информационного пространства невозможно. Поэтому развязки возможны только на пути заключения разумных соглашений, опирающихся на международное право и минимизирующих угрозы применения информационного оружия. Такие соглашения, как реальный вклад, в международное право могли бы только укрепить национальную безопасность подписавших их государств. При этом может оказаться даже полезным опыт компромиссов и соглашений, накопленный в политике предотвращения ракетно-ядерной войны и установления стратегической стабильности и баланса сил общего назначения в Европе.

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

АИС — автоматизированная информационная система
АТС — автоматическая телефонная станция
ВВП — валовой внутренний продукт
ВВС — военно-воздушные силы
ВМС — военно-морские силы
ВС — Вооруженные Силы
ГА ООН — Генеральная Ассамблея Организации Объединенных Наций
ДОВСЕ — Договор об обычных вооруженных силах в Европе
ИСЗ — искусственный спутник Земли
КОКОМ — Координационный комитет по многостороннему экспортному контролю
МАГАТЭ — Международное агентство по атомной энергии
МГТС — Московская городская телефонная сеть
МИД — Министерство иностранных дел
ОБСЕ — Организация по безопасности и сотрудничеству в Европе
ОМУ — оружие массового уничтожения
ОИС — открытые информационные сети
ПВО — противовоздушная оборона
ПЗУ — постоянное запоминающее устройство
ПРО — противоракетная оборона
РКРТ — режим контроля за ракетной технологией
РЛС — радиолокационные станции
РЭБ — радиоэлектронная борьба
СМИ — средства массовой информации
СНВ — стратегические наступательные вооружения
ФБР — Федеральное бюро расследований (США)
ФСБ — Федеральная служба безопасности (РФ)
ЭВМ — электронно-вычислительные машины
ЮНИДИР — Институт ООН по проблемам разоружения
ЮНСИТРАЛ — Комиссия ООН по праву международной торговли (UNCITRAL — United Nations Commission on International Trade Law)

ПРИЛОЖЕНИЕ 1. ГЛОССАРИЙ

Терминология, используемая при анализе вопросов, относящихся к проблемам информационной войны, информационного оружия, информационной безопасности

Этот глоссарий содержит лишь часть терминологии, с которой приходится сталкиваться в литературе. Из общей значительной массы терминов, применяемых при анализе проблем информационной войны, информационного оружия и информационной безопасности, выбраны наиболее, с точки зрения авторов, характерные или вызывающие неоднозначность понимания. Приведены определения, считающиеся авторами наиболее адекватными значению определяемых понятий в том смысле как последние используются в данной монографии и в других источниках, позиция которых разделяется авторами.

Авторизация (разрешение) — определение типов действий, разрешонных данному *пользователю*. Обычно разрешение находится в контексте установления подлинности. Как только подтверждена подлинность *пользователя*, ему могут быть разрешены различные типы доступа или деятельности в соответствии с его *полномочиями*.

Атака Ethernet контролируемая — форма *атаки информационной*, направленной на основной поток сообщений в сети Ethernet (например, контролируя пачки, проходящие через маршрутизатор) и изменение порядка дальнейшего движения для сообщений определенного вида или с определенными признаками (например, содержащих конкретный пароль). Этот процесс может быть выполнен автоматическими специально встраиваемыми средствами или с использованием программ-*пересмешников*.

Атака активная — форма нападения на *ресурс информационный*, в результате которого фактически изменяются или уничтожаются хранимые или обрабатываемые в нем данные или другие элементы ресурса.

Атака асинхронная — форма *атаки информационной*, при которой используются преимущества динамических действий системы, особенно способность управлять выбором времени исполнения тех или иных действий.

Атака информационная — попытка предпринять *действия несанкционированные* в системе (сети) в обход или с разрушением

средств защиты. *Нападение активное* нарушает (изменяет или уничтожает) данные. *Нападение пассивное* освобождает (снимает ограничения доступа) данные. Синонимы: *нападение информационное*, *кибератака*.

Атака пассивная — форма нападения на *ресурс информационный*, при котором данные «освобождаются» от ограничений по доступу (см.: *доступ ограниченный*), накладываемых атакуемой системой, или изменяется порядок контроля доступа к данным.

Атака хакерская — атака на *систему информационную* (сеть) или какую-либо ее часть, выполненная отдельным лицом (хакером) или согласованной группой лиц. Наиболее часто используется тактика, которая позволяет *злоумышленнику* узурпировать сессию *пользователя уполномоченного* для собственных, как правило, криминальных целей. Синоним: *налет хакерский*.

Аутентификация — положительная процедура установления пользователя, устройства или другого активного элемента в *системе информационной* по его заявленным полномочиями и паролю, иногда с использованием других, в частности, биометрических характеристик или предъявляемых электронных ключей.

Безопасности информационной концепция — совокупность официальных взглядов на обеспечение *безопасности информационной*, методы и средства защиты жизненно важных интересов личности, общества и государства в информационной сфере.

Безопасности информационной обеспечение — система мер и норм, нацеленная на поддержание *безопасности информационной*. Осуществляется по следующим направлениям: *организационное*, *нормативно-правовое*, *технологическое* и *кадровое*.
В составе системы обеспечения *безопасности информационной* могут создаваться подсистемы (системы), ориентированные на решение задач по отдельным направлениям обеспечения *безопасности информационной*.
Система обеспечения *безопасности информационной* государства является частью системы обеспечения его национальной безопасности.

Безопасности информационной обеспечение кадровое — система подготовки, переподготовки и использования кадров в интересах субъектов обеспечения *безопасности информационной*.

Безопасности информационной обеспечение нормативно-правовое — совокупность правовых норм, регулирующих отношения в области противодействия угрозам *безопасности информационной* и установленных государством механизмов реализации этих норм.

Безопасности информационной обеспечение организационное — упорядоченная по полномочиям и взаимодействию и установленная законом совокупность субъектов обеспечения *безопасности информационной*.

Безопасности информационной обеспечение технологическое — совокупность методического обеспечения и технологического инструментария, используемых субъектами обеспечения *безопасности информационной* в интересах выполнения возложенных на них функций по противодействию угрозам этой безопасности. Методическое обеспечение представляет собой совокупность методик, специальной и учебной литературы по решению частных задач обеспечения *безопасности информационной*. Методическое обеспечение, как правило, ориентируется на использование того или иного технологического инструментария. Технологический инструментарий представляет собой проблемно-ориентированную совокупность технических, программных, программно-технических и информационных средств.

Безопасности информационной системы нарушение (акции) — нарушение средств управления специфической частью *системы информационной*, отвечающей за контроль *целостности информации* и доступа к системе. Может быть как преднамеренное в результате неправомерных действий *злоумышленника*, так и в результате сбоя в работе отдельных программ или технических компонентов системы. В любом случае следствием является облегчение доступа к информации или *информации нарушение* в результате неверной (неконтролируемой) работы программного обеспечения защиты данных от изменений.

Безопасности информационной угроза — фактор или совокупность факторов, создающих опасность функционированию, сохранению и развитию *пространства информационного*.

Безопасность — 1) меры, принимаемые для защиты от всех действий, разработанных (предназначенных) для нанесения ущерба или снижения эффективности функционирования объекта или системы;
2) состояние, которое следует из внедрения и применения мер, которые гарантируют защиту от противоправных действий или влияний.

Безопасность информационная — 1) состояние защищенности основных интересов личности, общества и государства в *пространстве информационном*, включая *инфраструктуру информационно-телекоммуникационную* и собственно *информацию* в отношении таких ее свойств, как *целостность*, *объективность*, *доступность* и *конфиденциальность*;
2) совокупное состояние:
— *пространства информационного*, при котором обеспечивается его формирование и развитие в интересах граждан, организаций и государства;
— *инфраструктуры информационной*, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему (объект) при ее использовании;
— *информации*, при котором исключается или существенно затрудняется нарушение таких ее свойств, как *конфиденциальность*, *целостность* и *доступность*;
3) защищенность информационной среды личности, общества и государства от преднамеренных и непреднамеренных угроз и воздействий.

Безопасность информационная международная — состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в *пространстве информационном*.

Безопасность коммуникаций — защита (состояние защищенности), основанная на реализации совокупности разработанных (предназначенных) мер, предотвращающая *доступ неправомочный* к коммуникациям, а также исключающая *неправомерное использование информации*, в них циркулирующей, в любых целях. Включает как компоненты защиту *средств передачи данных технических* и защиту передаваемых данных, в том числе *криптозащиту*.

Безопасность компьютерная — защита АИС с использованием мер и средств (организационных и программно-технических), которые гарантируют *конфиденциальность*, *целостность* и *пригодность* информации, хранимой и обрабатываемой с использованием компьютерных средств; они включают технологию, процедуры, и аппаратные средства ЭВМ и компоненты программного обеспечения, необходимые для защиты систем вычислительных комплексов и информации, обрабатываемой, хранимой и передаваемой как внутри

системы так и от нее к другим информационно-вычислительным системам.

Безопасность систем информационная — синоним: *безопасность компьютерная*.

Безопасность электроники — составная часть *безопасности компьютерной* и *безопасности коммуникаций*, связанная с обеспечением правомерности деятельности электронных средств, включаемых в компьютерные и коммуникационные системы, соответственно.

Бомба двойная (вилочная) — разрушающий программный элемент, применяемый в основном к Unix-основанным системам, который инициирует безудержный процесс разделения и повторения (копирования) операционных процессов, что приводит к деградации производственных возможностей системы или (если насыщенность достигнута) полностью исключает возможность нормального функционирования системы.

Бомба логическая — обобщающий термин деструктивных программных комплексов (см.: *вирус программный*, *«троянский конь»*, *«часовая мина»*), резидентно находящихся на компьютере «жертвы» и активирующихся по определенному логическому условию (например, достижение определенной даты или набора определенных состояний системы). Наиболее известным и распространенным является срабатывание логической бомбы на заранее заданный контекст (ключевое слово). Может быть самостоятельной программой или фрагментом кода, распространяемым программистами или производителем некоторого программного продукта (пакета программ). Используется для инициирования вирусной или иного рода программной *атаки* на компьютерную систему. Механизм разрушающего воздействия может быть сколь угодно различным.

Бомба почтовая — деструктивный программный комплекс, способный передаваться с почтовыми (e-mail) сообщениями и активироваться на сервере или рабочей станции адресата. Как правило, нацелены на уничтожение информации на рабочей станции, но существуют примеры *бомб почтовых*, предназначенных для нарушения работы сетей или отдельных их элементов. Чаще используется в Unix-основанных системах.

Бомба-письмо — синоним: *бомба почтовая*.

Борьба радиоэлектронная (РЭБ) — любые военные действия, связанные с использованием электромагнитной и направленной энергии, в целях контроля над средствами электромагнитного спектра или нападения на противника. К трем главным подразделам РЭБ относятся *нападение радиоэлектронное*, *защита радиоэлектронная*, *поддержка средствами РЭБ*.

Вандал — в отличие от *кракера* и *хакера* этот термин используется в отношении действующих в *киберпространстве злоумышленников*, ставящих целью своих акций уничтожение *массивов информационных* и/или *систем информационных*. Отличительной их особенностью можно считать то, что в своих действиях они исходят из того, что противник знает о их *нападении*. Возможно, это определяется тем, что их целями являются специфические организации.

Век информационный — широко используемый, но не имеющий устоявшегося определения термин. В связи с этим рядом исследователей оспаривается правомерность выделения такого понятия как самостоятельного. Чаще всего под ним понимается начавшийся период времени, когда *системы информационные* стали неотъемлемой частью всех систем управления и жизнеобеспечения государства и общества. Термин вообще описывает предполагаемую эру, в которой информационной технологии становятся доминирующим техническим средством.

Взрыв информационный — резкий количественный и качественный скачек в сфере информации и коммуникации, вызванный научно-техническим прогрессом.

Виртуальное поле боя — применяется в военном контексте как эфир, занятый импульсами коммуникаций, базами данных, компьютерными сообщениями. В этом использовании, синонимичен *киберсреде*, *киберпространству*, *инфосфере*.

Вирус программный — обобщенный термин, определяющий фрагмент программного кода, способный самокопироваться («размножаться») путем записи своей копии в коды других программ компьютерной системы, подвергающейся компьютерному проникновению, разработанный (предназначенный) для негативного воздействия на

информацию или программное обеспечения компьютерной системы, скрываясь как часть другой программы. Активируется при запуске программы, в которую он внедрен, после чего может либо скопировать себя в другую программу, либо выполнить действия по искажению данных или нарушению работоспособности системы. Отличается способностью передаваться с другими программами практически любых видов, часто способностью самокопирования и самовоспроизводства в других системах, с которыми инфицированная система взаимодействует.

Вмешательство в информационно-телекоммуникационные системы и информационные ресурсы несанкционированное — вмешательство в процессы сбора, обработки, накопления, хранения, отображения, поиска, распространения и использования информации с целью нарушения нормального функционирования систем или нарушение *целостности*, *конфиденциальности* и *доступности* информационных и телекоммуникационных ресурсов.

Воздействие информационное — акт применения *оружия информационного*, а также непосредственное воздействие на элементы *пространства информационного* противника иными методами с целью нанесения ущерба.

Воздействие информационное прямое — изменение или уничтожение информации противника без использования специальных информационных средств.

Воздействие информационно-психологическое — *действия психологические*, осуществляемые с прямым или опосредованным использованием *средств информационно-психологических*.

Воздействие информационно-энергетическое — воздействие на биосистемы, и прежде всего на человека, физических полей различной природы, модулированных семантическими (смысловыми) сигналами, воспринимаемое биологическими организмами, а также средой их обитания в форме сигналов, сообщений, сведений, образов (т.е. в виде некоторой информации).

Воздействие на информационное пространство силовое — *нарушение* с использованием *оружия информационного* нормального (установленного законными собственниками, владельцами и пользователями) функционирования *инфраструктуры общества*

информационной, правил формирования, хранения и распространения информации и информационных ресурсов.

Воздействия информационного средства — 1) совокупность специальных лингвистических, программных, технических и иных средств, обеспечивающих извлечение, искажение или разрушение *информации*, *потоков информационных* или *ресурсов информационных*;
2) в информационных операциях эффективное использование *информации*, *систем информационных* и технологий в целях усиления средств и сил при осуществлении стратегии *операций информационных*.

Война третьей волны — синоним: *война информационная, война знаний*. Намек на «третью волну» экономической деятельности, которая концентрируется на информации и знании как предмете и результате труда.

Война знаний — синоним: *война информационная* или *война третьей волны*.

Война информационная — 1) *противоборство информационное* между государствами в *пространстве информационном* с целью нанесения ущерба *системам информационным*, процессам и ресурсам *структур критически важных*, подрыва политической, экономической и социальной систем, а также массированной психологической обработки населения с целью дестабилизации общества и государства;
2) особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии *силового воздействия на информационную сферу* этих государств.

Выделяются следующие разновидности *войны информационной*: подавление и уничтожение систем управления противоборствующей стороны, информационное обеспечение боевых действий, электронное подавление, психологическое воздействие, хакерская война, война в области экономической информации и кибернетическая война.

Подавление и уничтожение систем управления противоборствующей стороны — направлено на физическое уничтожение командных пунктов противника, нарушение управления его силами и средствами.

Информационное обеспечение боевых действий — нацелено на максимально полное предоставление и использование в системах управления войсками и оружием информации, собираемой интегрированными информационными системами в ходе военных действий.

Электронное подавление — имеет целью нарушение функционирования физических каналов распространения информации в информационной инфраструктуре противоборствующей стороны и вскрытие ее системы криптографической защиты. В рамках электронного подавления различают технические и криптографические операции. Технические операции электронного подавления ориентированы на вывод из строя приемо-передающих комплексов противоборствующей стороны, а криптографические операции — на вскрытие и подавление семантической составляющей передаваемой информации.

Психологическое воздействие — направлено против человеческого разума, а также компьютерной поддержки процессов принятия человеком ответственных решений. Выделяется четыре разновидности этого направления *войны информационной*: операции против населения; операции против руководящего состава войск; операции против живой силы противоборствующей стороны; операции по модификации культуры.

Хакерская война — имеет целью проникновение в телекоммуникационные и информационные системы противоборствующей стороны и нанесение ущерба этим системам и находящимся в них информационным ресурсам.

Война в области экономической информации — ориентирована на нанесение ущерба экономике противоборствующей стороны путем осуществления экономической блокады или информационной агрессии. При этом под *агрессией информационной экономической* понимается монопольное владение значительной частью информационных ресурсов и доминирование с элементами диктата на рынке информационных услуг.

Кибернетическая война — имеет целью нанесение ущерба информационным ресурсам противоборствующей стороны. Эта разновидность насильственных действий может быть реализована в виде: информационного терроризма, проявляющегося в виде разрозненных случаев насилия в отношении специально выбранных целей; информационных атак, направленных на изменение алгоритмов работы информационных систем при сохранении видимости нормального функционирования; демонстрации силы, направленной на внушение противоборствующей стороне требуемого представления о возможных последствиях применения против нее того или иного оружия; виртуализации реального мира.

Война информационная косвенная — изменение информации противника, создание явлений, которые противник должен наблюдать, анализировать и учитывать в своих стратегических и тактических действиях.

Война информационная экономическая — применение тактики *войны информационной* к основным процессам в экономическом пространстве.

Война информационно-основанная — подход к вооруженному конфликту, сосредоточивающийся на управлении и использовании информации во всех формах и на всех уровнях с тем, чтобы достичь решающего военного преимущества. Синонимы: *война информационная*, *война знаний*, *война третьей волны*, *война постиндустриальная*.

Война инфраструктурная — действия, направленные на деградацию, нарушение или разрушение фундаментальной инфраструктуры противника без обязательного прямого поражения живой силы, т.е. направленные против систем управления и жизнеобеспечения государства противника — тех его элементов, активов и структур, которые обеспечивают материальные и организационные основы целевых действий противника. В современных условиях практически неотделима от *войны информационной*.

Война инфраструктурная информационная — термин, по сути, сводимый к объединению *войны инфраструктурной* и *войны информационной* и подразумевающий активные действия против *ресурса информационного* фундаментальных инфраструктур государства противника, а также психологическое воздействие на его население.

Война компьютерная — синоним: *война сетевая*.

Война навигационная — действия, направленные на сокращение, изменение или лишение противника способности отслеживания географического местоположения и управления (т.е. навигации), основанного на таких способностях. Рассматриваются как часть методов *войны информационной*, относящихся к воздействию, в частности, на глобальную систему позиционирования (GPS), сеть навигационных спутников, наземные/бортовые навигационные приборы.

Война постиндустриальная — синоним: *война информационная*, *война знаний*, *война третьей волны*.

Война психологическая — 1) использование *пропаганды* и других *действий психологических*, имеющих первичную цель влияния на мнения, эмоции, отношения, и поведение отдельных личностей, групп людей и население противника таким способом, чтобы поддержать достижение целей войны;

2) *действия психологические*, направленные на решение политических, военных, экономических и идеологических задач с целью создавать в отношении враждебного государства эмоции, отношения или поведение, способствующие достижению своих целей.

Война радиоэлектронная — синоним: *борьба радиоэлектронная* (РЭБ).

Война с применением оружия направленной энергии — боевые действия с использованием *направленной энергии оружия*, и контрмеры в целях либо нанесения непосредственного ущерба или уничтожения оборудования, объектов и личного состава противника, либо в целях обнаружения, использования в своих интересах, снижения мощности или предотвращения применения электромагнитного спектра с помощью нанесения ущерба, уничтожения и дезорганизации. Сюда также относятся действия, предпринимаемые в целях защиты своих оборудования, объектов и личного состава и сохранения возможностей использования своих средств электромагнитного спектра.

Война сетевая — 1) принцип организации ведения военных действий, при котором силы и средства организуются не по принципу иерархического подчинения, а по принципу сети, соответственно меняется и принцип организации управления. Такой принцип традиционно используется крупными террористическими организациями. Применялся он и в партизанских движениях. Сетевой принцип используется хакерскими группами. Многие аналитики считают его основным в *войне информационной*;
2) синоним: *война компьютерная*.

Война систем информационная — подкатегория *войны информационной*. *Война систем информационная* нацелена на системы обработки информации, каналы и средства передачи информации, прекращение или нарушение деятельности которых обеспечивает тактическое и стратегическое преимущество.

Восприятие — процесс отражения действительности в форме чувственного образа объекта, иначе — процесс оценки *информации*, которая была получена и классифицирована пятью физическими чувствами (зрение, слух, обоняние, вкус и осязание) и интерпретировался в соответствии с критериями культуры и общества.

Восприятием управление — в данном контексте следует относить к методам *воздействия информационно-психологического*. Действия,

сводящиеся к передаче или селектированию *информации* и индикаторов восприятия и имеющие целью влиять на эмоции, поводы и объективное рассуждение субъектов восприятия. Нацелено, в первую очередь на интеллектуальную элиту общества страны противника и лидеров всех уровней с тем, чтобы влиять на официальные оценки, в конечном счете заканчивающиеся официальными действиями, благоприятными целям субъекта *восприятием управления*. Различными способами *восприятием управление* комбинирует проектирование правды, безопасность действий, сокрытие и обман, а также специальные психологические действия.

Вторжение — в данном контексте — *доступ неправомочный* или *проникновение* любого рода (физическое или информационное) в компьютеры, информационные системы и сети непосредственно или опосредованно через корреспондирующие сети или системы. Синонимы: *проникновение*, *доступ неправомочный*.

Вторжение электромагнитное — намеренное воздействие электромагнитной энергией на процессы обработки или передачи информации любым способом с целью их нарушения, изменения, в том числе изменения или нарушения обрабатываемой или передаваемой информации, обмана операторов или внесения беспорядка в организационные структуры обработки и передачи информации. Может являться элементом *войны радиоэлектронной*.

Вторжения обнаружение — 1) фиксация факта *вторжения*, в том числе *вторжения электромагнитного* по каким-либо признакам;
2) процесс (действия) определения признаков, дающих основание сделать заключение о совершении *вторжения*, в том числе *вторжения электромагнитного*.

Вторжения обнаружения система — программное обеспечение и/или система аппаратных средств ЭВМ, разработанная (предназначенная) для контроля технико-программных средств компьютера, информационной системы или сети с целью идентификации признаков *вторжения попытки*.

Вторжения попытка — действия, направленные на осуществление *вторжения*, однако по какой-либо причине не завершенные или не приведшие к собственно *вторжению*. Однако уже на этом этапе может представлять опасность и привести к нежелательным последствиям в зависимости от использовавшихся методов и стадии завершенности *вторжения попытки*.

Гарантия информационная — 1) мера уверенности (доверия), что особенности системы безопасности (проводимые акции) и архитектура информационной системы (сети) точно отражают и обеспечивают принятую политику безопасности системы (сети);
2) *операции информационные оборонительные*, которые охраняют и защищают информацию и *системы информационные*, обеспечивая их *доступность*, *целостность*, *достоверность*, *конфиденциальность* и невозможность ее отрицания. Сюда относится обеспечение восстановления информационных систем с помощью привлечения возможностей по защите, обнаружению и реагированию.

Глобальная информационная окружающая среда — полная общемировая совокупность *пространств информационных* и *ресурсов информационных*.

Дампстер — методика анализа уничтожаемой пользователем информации с целью определения его идентифицирующих признаков для последующего их использования в незаконных целях, в частности, для проникновения в *массивы информационные* или совершения иных действий от имени данного пользователя (см.: *спуфинг*).

Данные — в данном контексте: представление фактов, суждений (знаний), или указаний формализованным способом в виде знаков или аналоговых сигналов, подходящим для связи, интерпретации или обработки автоматизированными средствами, а также восприятием человеком в любой доступной форме.

Данные персональные — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие (способствующие) идентифицировать его личность.

Данные — управляемое нападение — форма нападения (*атака*), при котором агрессивный программный блок внедряется в форме внешне безвредных данных, подготовленных от имени официального пользователя или в ходе штатной работы программного обеспечения, что позволяет преодолевать защитные системы информационных сетей типа *фаэвол* и начинать атаку против поражаемой системы уже «позади» *фаэвол*.

Двойная конвертация — представление информации в виде содержания и конверта сообщения в новом внешнем конверте, с целью ее защиты

всякий раз, когда сообщение отправлено через недостаточно надежную область информационной сети. Содержание нового внешнего конверта может быть зашифровано в зависимости от степени доверия к конкретному сетевому трафику.

Деградация обслуживания — любое сокращение (относительно норм или ожиданий) в реакции процессов обслуживания: увеличение времени ответа, снижение количественной производительности или параметров качества. Этот термин часто используется, чтобы обозначить общий набор видов ухудшения обслуживания, которое в крайнем варианте (полная деградация) составляет полный отказ от обслуживания.

Дезинформация — 1) меры, направленные на введение в заблуждение противника с помощью подтасовки, искажения или фальсификации информации, вынуждающие его действовать в ущерб своим интересам; 2) заведомо ложные сведения, распространяемые или передаваемые с целью введения в заблуждение.

Дезинформация техническая — создание ложной информации об объекте защиты путем воспроизведения несуществующих или искажения действительных демаскирующих признаков.

Действия неправомочные — действия в отношении *ресурса информационного*, совершаемые в нарушение правил и полномочий (санкций), установленных для данного ресурса.

Действия несанкционированные — синоним: *действия неправомочные*.

Действия психологические — запланированные действия, направленные на доведение специально отобранной информации и индикаторов потребителю (конкретным субъектам, группам, населению) с тем, чтобы повлиять на его эмоции, поводы, цели, рассуждения и в конечном счете поведение противника (его правительства, организаций, групп и индивидуумов). Вспомогательная цель может состоять в том, чтобы стимулировать или укрепить у противника отношения и поведение, благоприятные для целей субъекта *действия психологического*. Синоним: *операции психологические*.

Действия психологические стратегические — *действия психологические*, проводимые с широкими или долгосрочными целями в координации с общим стратегическим планированием, с постепенными

результатами, осуществимыми в будущем. Направлены на руководящие круги, командование, личный состав вооруженных сил и гражданское население противника в его тылу или прифронтовой полосе позади боевых зон или на аналогичные круги дружественных противнику или нейтральных стран.

Диверсия информационная — криминальное действие, по объективным признакам схожее с *кибертерроризмом*, однако в качестве цели имеющее подрыв экономической безопасности и обороноспособности.

Доведение сведений — вид *действия психологического*. Доведение через СМИ или по другим каналам информации до субъекта, группы или общества с целью убедить объект воздействия (индивидуума или группу) изменить или сформировать мнения, эмоции, отношения и форму поведения, а в конечном итоге предпринять конкретные поступки в заданных интересах.

Доминирование инструментальное — (в противоположность *доминированию информационному* в данном контексте) — подавляющее преимущество, полученное за счет превышающих технических возможностей (силы) относительно любой формы передачи данных в уместных информационных действиях.

Доминирование информационное — подавляющее преимущество, полученное через превышающую эффективность информационной деятельности (приобретение и использование данных, информации, знаний) в такой степени, что это преимущество демонстрируется практически через превышающую эффективность инструментальной деятельности.

Доступ контрактный — преднамеренное указание неверных данных при заключении контракта или невыполнение абонентом информационной сети или сети связи контрактных условий оплаты.

Доступ несанкционированный — синоним: *доступ неправомочный*.

Доступ неправомочный — доступ к *ресурсу информационному*, совершаемый в нарушение правил и полномочий (санкций), установленных для данного ресурса.

Доступ ограниченный — доступ к *ресурсу информационному*, разрешаемый только определенному установленными для данного ресурса правилами и полномочиями (санкциями) кругу лиц.

Доступ неправомерный как вид мошенничества — несанкционированное использование услуг связи, неправомочный и преднамеренный доступ абонента к услугам связи с целью личной или коллективной выгоды.

Доступ технический — неправомочное изготовление (клонирование) телефонных трубок или платежных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платежных отметок.

Доступ фрикерсткий — проникновение в телекоммуникационную сеть для получения информации обмена кодами доступа, их изменения и использования в своих целях, взлом системы защиты.

Доступа несанкционированного предпосылки — совокупность факторов, создающих благоприятные условия для *доступа несанкционированного*.

Доступность — характеристика информации, определяющая возможность ее получения пользователем информационной системы. Выделяют *информацию открытую* (общедоступную) и *информацию ограниченного доступа*.

Задняя дверь — 1) дополнительная точка входа в операционной системе или другом базовом программном обеспечении компьютерной информационной системы, позволяющая пройти в процесс обработки информации в обход средств обеспечения безопасности системы, преднамеренно встроенная проектировщиками или разработчиками программных средств. Синоним: *люк*, *черный ход*.
2) скрытое программное обеспечение или механизм аппаратных средств ЭВМ, предназначенные для обхода средств обеспечения безопасности.

Зашиты информации системы — система мер и действий, направленных на обеспечение *информации безопасности* с использованием всех возможностей *защиты информации инфраструктуры*.

Защита информационная — совокупность информационных средств, обеспечивающих (предназначенных для) противодействие *воздействию информационному*, включая *атаки информационные*, а также реализуемым на каналах распространения информации (СМИ, сети передачи данных и т.п.) *действиям психологическим*.

Защита радиоэлектронная — раздел РЭБ, включающий действия, предпринимаемые для защиты личного состава, объектов и оборудования от любых последствий применения средств РЭБ своими войсками или противником, ведущих к снижению эффективности, нейтрализации или уничтожению боевых возможностей своих войск.

Защиты информации инфраструктура — разделенная или связанная совокупность компьютеров, коммуникаций, данных, технологий и систем безопасности, систем обучения, обеспечения, использования и подготовки кадров и других структур поддержки всех форм *безопасности информации* и информационных инфраструктур всех уровней для данного объекта, структуры, территории.

Злоумышленник — в данном контексте: лицо или группа лиц, преднамеренно совершающих *действия неправомочные* с использованием штатных или специальных технически-программных средств.

Зондаж — любое усилие, направленное на сбор информации относительно технических средств или пользователей информационной системы (сети), для цели получения *доступа неправомочного* к системе (сети).

Идентификация — процедура проверки идентичности пользователя, устройства или другого активного элемента в *системе информационной* в соответствии с его фактическими и заявленными полномочиями и парольной системой (иногда с использованием других, в частности биометрических характеристик), часто рассматривается как условие разрешения доступа к ресурсам в системе.

Идентифицируемость пользователя — принцип доступа к информационной системе (сети), подразумевающий, что индивидуумы, использующие средство, систему или сеть должны быть идентифицируемы. Вводится с целью обеспечения правомочности доступа к системе (сети), а также возможности выявления и привлечения к ответственности нарушителей требований безопасности работы системы (сети) и обрабатываемой ею информации.

Инфократия (киберкратия) — термин, еще не достаточно определенный и распространенный. Ассоциируется со способом правления или проведением политики, в которых информация и доступ в

глобальные информационные сети являются доминирующим источником полномочия. Этот термин, производный от корней «cyber-» и «-cracy», лингвистически означает управление посредством информации. Сторонники такой концепции исходят из того, что информация и управление на ее основе станут доминирующим источником власти, как естественный следующий шаг в политическом развитии общества. Трактуется, что принцип инфократии (киберкратии), являющийся порождением революции в информации и технологиях коммуникаций, может медленно, но радикально определить, кто управляет, как и почему.

Информатизации средства — технические, программные, лингвистические, правовые, организационные средства (средства вычислительной, множительной и пр. предназначенной для обработки и размножения информации и информационных материалов техники, компьютерные программы, словари, тезаурусы и классификаторы, инструкции и методики, положения, уставы, должностные инструкции, эксплуатационная и сопроводительная документация), используемые или специально создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информации защита — совокупность организационных, правовых, технических и технологических мер по предотвращению и отражению угроз *ресурсам информационным* и *системам информационным*, устранению их последствий.

Информации массовой средства — периодические печатные издания, радио-, теле-, видеопрограммы, кинохроникальные программы и иные формы непрерывного или периодического распространения массовой информации. При этом предполагается, что периодическое печатное издание (газета, журнал, альманах, бюллетень) должно иметь постоянное название, текущий номер и выходить в свет не реже одного раза в год.

Информации разрушение — полная потеря хранящихся в информационных системах или передаваемых по информационным сетям данных или их изменение, исключающее возможность правильной их интерпретации и восстановления.

Информации утечка — совершившийся факт разглашения (распространения) *информации ограниченного доступа* за пределами санкционированного круга лиц в результате совершенных *действий неправомочных*.

Информации уязвимость — свойство хранимых, обрабатываемых и передаваемых данных, массивов и документов, при котором имеется потенциальная возможность их утечки, физического разрушения и несанкционированного использования.

Информационного века оружие — синоним: *оружие информационное*.

Информационной безопасности угроза — факторы, создающие опасность основным интересам личности, общества и государства в информационном пространстве.

Информация — 1) сообщение, осведомление о положении дел, сведения о чем-либо, передаваемые людьми;
2) уменьшаемая, снимаемая неопределенность в результате получения сообщений;
3) сообщение, неразрывно связанное с управлением, сигналы в единстве синтаксических, семантических и прагматических характеристик;
4) передача, отражение разнообразия в любых объектах и процессах (неживой и живой природы);
5) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы предоставления.

Информация бытовая — сведения, возникающие в процессе обыденного человеческого общения.

Информация в войне / информация в военных средствах — термин, который обозначает применение информации и информационных технологий в контексте ведения военных действий (традиционно понимаемых), вне ассоциации с информационной войной и информационным оружием.

Информация документированная — *информация*, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать.

Информация конфиденциальная — сведения ограниченного доступа, не отнесенные к государственной тайне. К *информации конфиденциальной*, в частности, относятся сведения, составляющие служебную и коммерческую тайны, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, личную и семейную тайну, а также сведения, раскрывающие частную жизнь граждан.

Информация критическая — определенные факты относительно намерений, способностей и действий, жизненно необходимых для эффективного управления и деятельности *структур критически важных*, эффективного выполнения стоящих стратегических задач.

Информация ограниченного доступа — вид сведений, доступ к которым ограничен в соответствии с законодательством и разглашение которых может нанести ущерб интересам других лиц, общества и государства. В составе такой информации различают сведения, составляющие государственную тайну, и *информацию конфиденциальную*.

Информация открытая — общедоступные сведения, не имеющие ограничений по доступу к ним всех заинтересованных лиц.

Информация развлекательная — сведения, предназначенные для использования человеком в основном в процессе отдыха. К информации такого рода следует отнести прежде всего произведения художественной литературы, концертные программы, кинофильмы, телепередачи и т.д.

Информация распорядительная — сведения, возникающие в связи с реализацией человеком некоторых нормативных предписаний, инструкций: заполнение служебных журналов, управление движением автотранспорта, производственным станом и пр.

Информация служебная — сведения, появляющиеся в связи с реализацией функций государственной службы. Круг сведений, составляющих *информацию служебную*, весьма широк и охватывает все сферы деятельности органов государственной власти.

Информация социально-значимая — сведения об интересующих значительное количество людей событиях общественной жизни внутри страны и за рубежом, деятельности политических партий и движений, лидеров общества и государства, рынке труда и капитала и т.д., кроме некоторых наиболее общих сведений о состоянии экономической сферы.

Информация частная — сведения, раскрывающие реализацию гражданином своих личных конституционных прав на свободу мысли, совести, собраний, информационной деятельности, о его мировоззрении, нравственных *ценностях*, отношении к религии и т.д. Как правило, затрагивает ограниченный круг лиц и касается их частной жизни.

Информация экономическая — до конца не определенный (в связи с неопределенностью термина экономика) термин, затрагивающий весьма широкий круг фактов, процессов, явлений и лиц, задействованных в деятельности объектов хозяйствования, производственных предприятий, финансовых и кредитно-денежных организаций, включая инвестиционные процессы. К *информации экономической* может быть отнесена коммерческая информация и реклама.

Инфосфера — см.: *пространство информационное*.

Инфраструктура информационная — технические средства и системы формирования, обработки, хранения и передачи информации. Является средой, которая обеспечивает возможность сбора, передачи, хранения, автоматизированной обработки и распространения информации в обществе.

Инфраструктура информационная глобальная — всемирная взаимосвязь сетей связи, компьютерной техники, баз данных и бытовой электроники, делающая доступной для пользователей обширные объемы информации. Охватывает широкий спектр оборудования, включающий камеры, сканеры, клавиатуры, факсы, компьютеры, коммутаторы, компакт-диски, видео- и аудиопленки, провода, кабели, спутники, волоконно-оптические линии передач, сети всех типов, телевизоры, мониторы, принтеры и многое другое.

Инфраструктура информационная национальная — единая или взаимосвязанная система компьютерной техники, линий связи, использования данных, безопасности, личного состава, обучения и других вспомогательных структур, обслуживающих местные, национальные и всемирные информационные нужды и функционирующих в интересах и масштабах государства.

Инфраструктура информационная общества — совокупность *систем информационно-телекоммуникационных* и *связи сетей*, индустрии средств информатизации, телекоммуникации и связи; системы формирования и обеспечения сохранности информационных ресурсов; системы обеспечения доступа к *средствам информационно-телекоммуникационным*, *связи сетям* и *ресурсам информационным*; *информационных услуг индустрии* и *рынка информационного*; системы подготовки и переподготовки кадров, проведения научных исследований.

Инцидент — при проведении информационных операций — проанализированный случай попытки получения *доступа несанкционированного* или *нападения информационного* на автоматизированную информационную систему. Он включает несанкционированное зондирование и просматривание; прерывание или воспрещение обслуживания; искаженный или уничтоженный ввод, обработку, хранение или вывод информации; или внесение изменений в характеристики аппаратного оборудования, программно-аппаратных средств или программного обеспечения информационной системы с (или без) ведома, инструкции или намерения пользователя.

Использование информации неправомерное — передача, распространение (публикация), применение в *действиях информационных* полученных легальным путем сведений в нарушение правил и полномочий (санкций), установленных для данных сведений и субъекта, предпринявшего такие действия.

Использование информационно-телекоммуникационных систем и информационных ресурсов неправомерное — использование телекоммуникационных и информационных систем и ресурсов без соответствующих прав или с нарушением установленных правил, законодательства или норм международного права.

Капля — «двоичный большой объект», используемый для описания любой случайной большой совокупности частиц, обычно картина или звуковой файл. Нередко используется как умеренная угроза хакера при отправлении по электронной почте (*бомба почтовая*). Может также использоваться, чтобы скрыть *бомбу логическую*.

Кибератака — см.: *атака информационная*.

Киберпространство — наиболее часто употребляемый из ряда синонимов, к которым следует отнести термины типа: *киберсреда*, *инфосфера*, а также чисто англоязычный datasphere. См.: *пространство информационное*.

Киберсреда — синоним: *киберпространство*.

Кибердиверсия — синоним: *диверсия информационная*.

Кибертерроризм — синоним: *терроризм информационный*.

Командование и управление — в военном приложении: осуществление власти и руководства соответствующим образом назначенным командиром над подчиненными и приданными подразделениями в целях выполнения поставленной задачи. Функции командования и управления выполняются посредством организации личного состава, оборудования, средств связи, объектов и методик, используемых командиром при планировании, руководстве, координации и управлении силами и операциями в целях выполнения поставленной задачи.

Командования и управления боевое применение — комплексное использование мер обеспечения секретности операций, военной дезинформации, психологических операций, средств РЭБ и физического уничтожения при взаимной поддержке разведки в целях не допустить разглашения информации, оказать влияние, снизить эффективность или уничтожить средства командования и управления противника, в то же время осуществляя защиту своих средств командования и управления против таких действий. Боевое применение командования и управления представляет собой использование информационных операций. Бывает как наступательным, так и оборонительным.

Командования и управления боевое применение наступательное — комплексное использование мер обеспечения секретности операций, военной дезинформации, психологических операций, средств РЭБ и физического уничтожения, направленных против эффективного осуществления командования и управления сил противника посредством недопущения разглашения информации, оказания влияние, снижения эффективности и уничтожения системы командования и управления противника.

Командования и управления боевое применение оборонительное — комплексное использование мер обеспечения секретности операций, военной дезинформации, психологических операций, средств РЭБ и физического уничтожения, направленных на поддержание эффективного командования и управления своими войсками, используя свои преимущества и подавляя контрусилия противника по недопущению разглашения информации, оказанию влияния, снижению эффективности и уничтожению своей системы командования и управления.

Командования и управления система — средства обслуживания, оборудование, коммуникации, процедуры и персонал, необходимый для командующего для планирования, направления и действий управления назначенных сил в соответствии с установленными назначениями.

Командования и управления система, атака — синхронизированное выполнение действий, направленных на снижение эффективности функционирования *командования и управления системы*, воздействуя на информацию и информационные системы и сети противника.

Командования и управления система, средства воздействия — средства информационного воздействия, психологических действий, радиоэлектронной войны и физического разрушения, направленные на деградацию или уничтожение *командования и управления системы* противника, при защите своей аналогичной системы против таких действий. Применение данных средств может рассматриваться как часть *войны информационной* в военных действиях. Могут применяться во все периоды военных действий и на всех уровнях конфликта.

Командования и управления системы защита — обеспечение эффективности *командования и управления системы* собственных сил при противодействии усилиям противника, направленным на ее деградацию или уничтожение. Система может носить наступательный или защитный характер: наступательные средства используют *командования и управления системы*, *средства воздействия*, чтобы уменьшить способность противника провести атаку; оборонительная составляющая уменьшает уязвимость своей системы для средств противника за счет применения адекватных физических, электронных и информационных мер и средств.

Контрдезинформация — усилия по воспрещению, нейтрализации, уменьшению последствий или по извлечению выгод из операций противника по *дезинформации*.

Контрмеры информационные — действия, устройства, процедуры, техника или другие меры, которые снижают уязвимость автоматизированной информационной системы или информационной сети. Контрмеры, которые нацелены на определенные угрозы и уязвимость, вовлекают более активные методы, такие как *безопасность* и *защита информационная*.

Контролируемый пакет — прием *атаки*, при котором нападавшие тайно вставляют программу в отдаленных переключателях или хостах сети. Программа контролирует информационные пачки, посланные через сети, и посылает копию восстановленной информации *хакеру*. Анализируя полученные таким образом первые 125 символов связи, нападавшие

могут изучать пароли и идентификаторы пользователя, которые, в свою очередь, они могут использовать, чтобы проникнуть в системы.

Контроль — в данном контексте, тайное наблюдение и анализ потоков данных с целью перехватывать и захватывать годную для использования информацию. См.: *Ethernet контроль*, *пакет контролируемый*, *пароль контролируемый*.

Конфиденциальность (информации) — принцип обработки, хранения и доступа к информации, обеспечивающий нераскрытие ее любому не уполномоченному на доступ к ней лицу. Частично синонимичен с тайной.

Кракер — обобщенный термин, обозначающий любого, кто пытается проникнуть в информационные массивы или сети за счет взлома их систем защиты, вне зависимости от цели проникновения.

Криптоанализ — 1) раскрытие зашифрованного криптографическими методами текста с помощью известного ключа или без него (за счет вскрытия неизвестного ключа);
2) анализ криптографической системы и ее входных и выходных данных с целью определения засекреченных переменных и значимой информации, включая открытый текст.

Криптография — 1) наука об использовании математических методов и технических средств для преобразования открытой защищаемой информации в закрытую, зашифрованную форму, затрудняющую восстановления открытой информации;
2) тайнопись, система изменения информации (текста, речи) с целью сделать ее непонятной для непосвященных лиц.

Криптозащита — обобщенный термин для обозначения защиты информации методом ее шифрования.

Криптология — наука о безопасности (секретности) передачи информации; включает *криптографию* (шифрование) и *криптоанализ*.

Люк — скрытое программное обеспечение или механизм аппаратных средств ЭВМ, позволяющие обходить контроль безопасности систем, в которых они функционируют. Синонимы: *задняя дверь*, *черный ход*.

Массив информационный — специальным образом организованная совокупность *информации документированной* или хранимой в электронном контуре *системы информационной*.

Модуль проверки текущего состояния — программный инструмент перехвата потенциально годных для использования данных в процессе их продвижения по информационной сети. Используется *хакерами*, чтобы захватить идентификатор и пароли пользователя.

Мошенничество компьютерное — *компьютерное преступление*, предусматривающее преднамеренное введение в заблуждение или изменение данных, имеющее целью получение незаконного дохода в любой форме и совершаемое через или в отношении компьютеров и/или информационных сетей.

Мусорщик — *злоумышленник*, предпринимающий попытку по остаткам информационной деятельности восстановить чувствительные данные законного пользователя (идентифицирующие данные, пароли, сведения о полномочиях и т.п.) без его разрешения в целях последующего несанкционированного проникновения в систему (сеть) под его именем. См.: *дампстер*.

Налет хакерский — см.: *атака хакерская*.

Нападение — в данном контексте, акт, связанный с нанесением физического ущерба объекту *инфраструктуры информационной*.

Нападение информационное — см.: *атака информационная*.

Нападение на компьютерную сеть — операции, направленные на прерывание, воспрещение, снижение качества или уничтожение информации, находящейся в компьютерах или компьютерных сетях, или самих компьютеров и компьютерных сетей. Синоним: *атака*.

Нападение пассивное — *нападение информационное*, имеющее целью только открытие доступа к информации или информационным массивам без нанесения им прямого ущерба (изменения, уничтожения и пр.).

Нападение радиоэлектронное — раздел РЭБ, сопряженный с использованием электромагнитного оружия, *направленной энергии оружия* или оружия поражения излучающих радиоэлектронных систем

для нападения на личный состав, объекты или оборудование с целью снижения эффективности, нейтрализации или уничтожения боевых возможностей противника. *Нападение радиоэлектронное* включает: 1) действия, предпринимаемые для предотвращения или уменьшения эффективного использования противником электромагнитного спектра, такие как радиоэлектронное подавление и дезинформация с использованием радиоэлектронных систем; 2) использование оружия, в котором применяется электромагнитная или направленная энергия в качестве основного поражающего механизма (лазеры, радиочастотное оружие, пучки направленной энергии или оружие поражения излучающих радиоэлектронных систем).

Нападение техническое — нападение, которое может быть совершено, обходя или аннулируя аппаратные средства ЭВМ и механизмы защиты программного обеспечения с использованием специальных аппаратных средств.

Напевать — преднамеренно отправлять по электронной почте провокационные сообщения с намерением отвлечь других и втянуть в бессмысленную переписку.

Направленной энергии оружие — система, использующая направленную энергию прежде всего непосредственно для повреждения или уничтожения основного оборудования, вооружений, средств их обеспечения и обслуживания и личного состава противника.

Нарушение средств безопасности системы — успешное поражение средства управления безопасностью, которое завершается проникновением в систему. Нарушение средств управления специфической информационной системы, как правило, приводит к тому, что информационные активы или компоненты системы становятся доступны неуполномоченным на то лицам или программно-техническим средствам.

Нарушитель — в данном контексте: лицо или группа лиц, совершающих *действия неправомочные* с использованием штатных технико-программных средств.

НОРД-петля — «наблюдение, ориентация, решение, действия петля». Общий принцип организации работы на основе информации. Нарушение или повреждение НОРД-петли — обычный способ теоретического описания цели и/или главного результата *воздействия информационного*.

Обман — меры, разработанные (предназначенные), чтобы ввести в заблуждение противника манипуляцией, искажением или фальсификацией информации и тем самым стимулировать его реагировать способом, наносящим ущерб его интересам.

Обмен информационный международный — передача и получение информационных продуктов, а также оказание информационных услуг через государственную границу страны *ресурса информационного владельца*.

Обмена информационного международного средства — *инфраструктура информационная*, используемая при *обмене информационном международном*.

Обнаружение аномалии — обобщенный термин для класса тактик обнаружения *вторжения*, которые основаны на идентификации потенциальных *попыток вторжения* на основании их возможных аномальных по сравнению с ожидаемыми действий.

Общество информационное — 1) состояние развития общественных и прежде всего производственных отношений, при котором основная часть валового продукта производится не за счет материального производства, а на основе создания и продажи наукоемких технологий, информационных продуктов, т.е. результатов интеллектуального труда граждан, а также самой информации, порождаемой в качестве продукта труда;
2) общество, в котором основным предметом труда большей или значительной части людей являются информация и знания, а орудием труда — информационные технологии.

Объективность (информации) — свойство информации, определяющее ее соответствие реальным описываемым с ее помощью объектам, процессам, явлениям.

Операции информационные — действия любого характера, предпринимаемые для оказания воздействия на информацию и информационные системы (сети) противника при защите своей собственной информации и информационных систем.

Операции информационные наступательные — единое использование приданных и поддерживающих возможностей и действий,

поддерживаемых на взаимной основе разведкой, для оказания воздействия на руководство противника в целях достижения или развития конкретных задач. Эти возможности и действия включают, но не ограничиваются, обеспечением секретности операций, военным введением в заблуждение, психологическими операциями, операциями РЭБ, физическим нападением и/или уничтожением и специальными информационными операциями, а также могут включать нападение на компьютерную сеть.

Операции информационные оборонительные — интеграция и координация политики, методик, операций, личного состава и технологии в целях охраны и защиты информации и информационных систем. Оборонительные информационные операции осуществляются посредством *гарантий информационных*, обеспечения физической безопасности, оперативной безопасности, *контрдезинформации*, контрпсихологических операций, контрразведки, РЭБ и *информационных операций специальных*. *Операции информационные оборонительные* обеспечивают своевременный, четкий и соответствующий доступ к информации, в то же время не давая противнику возможности использовать свою информацию и информационные системы в своих целях.

Операции информационные специальные — информационные операции, которые в силу своего секретного характера, их возможного потенциального эффекта или воздействия, соображений безопасности или угрозы национальной безопасности требуют особого процесса рассмотрения и одобрения.

Операции психологические — синоним: *действия психологические*.

Оружие информационное — 1) средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам государства, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные системы государства, а также массированной психологической обработки населения с целью дестабилизации общества и государства;
2) специальные средства, технологии и информация, позволяющие осуществить «силовое» воздействие на информационное пространство общества и привести к значительному ущербу политическим, оборонным, экономическим и другим жизненно важным интересам государства;

3) комплекс технических и других средств и технологий, предназначенных для:
— установления контроля над информационными ресурсами потенциального противника;
— вмешательства в работу его систем управления и информационных сетей, систем связи и т.п. в целях нарушения их работоспособности, вплоть до полного выведения из строя, изъятия, искажения содержащихся в них данных или направленного введения специальной информации;
— распространения выгодной информации и дезинформации в системе формирования общественного мнения и принятия решений;
— совокупность специальных способов и средств воздействия на сознание и психику политического и военного руководства, личного состава вооруженных сил, спецслужб и населения противостоящего государства, используемых для достижения превосходства в информационном противоборстве.

Оружие информационное оперативное — совокупность видов *оружия информационного*, способного обеспечить решение важных задач при проведении операции вооруженных сил на определенном театре военных действий.

Оружие информационное стратегическое — совокупность видов *оружия информационного*, способного нанести неприемлемый ущерб политическим, экономическим и военным интересам страны, а также структурам, образующим ее стратегический потенциал, в рамках стратегической операции вооруженных сил государства.

Оружие информационное тактическое — совокупность видов *оружия информационного*, способного обеспечить решение важных задач в ходе боевых действий или боя.

Оружие психотронное — специальные *средства психотронные*, применяемые против живой силы и населения противника с целью решения военных задач.

Отказ в обслуживании — действие, которое отстраняет любую часть информационной системы (сети) от функционирования в соответствии с предназначенной целью. Может включать отказ услуг или процессов, ограниченных одной машиной. Однако термин наиболее часто используется в контексте действий, хоть и направленных против одного абонента (пользователя), но которые приводят к неспособности

исполнять функции по обслуживанию и других пользователей, особенно в рамках сети.

Отказ информационный, средства вызывающие — средства воздействия на информационные системы (сети) противника, приводящие к изменениям функций относительно целей системы. Имеются два типа такого воздействия: *нападение* на информационные системы противника, и внедрение *дезинформации* в системы с целью стимулировать противника к невыгодным ему действиям. В военных условиях для прямых нападений используют средства РЭБ, «забивающие» радиосвязь и каналы передачи данных.

Пароля взламывание — техника (способ) тайно получать доступ к информационной системе (сети), в которой нападавшие пробуют угадать (определить) или украсть пароли. Пользователи часто выбирают слабый пароль. Два главных источника слабости в паролях — легко предполагаемые пароли, основанные на знании пользователя (например, девичья фамилия жены) и пароли, которые являются восприимчивыми к раскрытию с использованием словаря как источника предположений. Эта техника была легко автоматизирована *хакерами*, компьютеры могут очень эффективно и систематически делать предположение. Например, если пароль — слово словаря, компьютер может быстро посмотреть все возможности.

Пересмешник — компьютерная программа или процесс, который, имитируя стандартные программы или процессы вычислительного комплекса, исполняет злонамеренные действия в отношении данного комплекса или связанных с ним в рамках локальной сети.

Пигбекинг — получение *доступа неправомочного* к системе через законно установленную связь (доступ) другого пользователя.

Поддержка средствами РЭБ — раздел РЭБ, включающий действия, выделенные в качестве задачи или находящиеся под непосредственным управлением оперативного командира, имеющие целью поиск, перехват, опознание и обнаружение источников намеренного или ненамеренного излучения электромагнитной энергии в целях немедленного распознавания целей. Таким образом, поддержка средствами РЭБ обеспечивает получение информации, необходимой для немедленного принятия решений, связанных с операциями с применением средств РЭБ и другими тактическими действиями, такими как меры по предотвращению

воздействия противника, выбор цели и самонаведение. Данные, получаемые в ходе поддержки средствами РЭБ, могут быть использованы в качестве информации разведки источников электромагнитных сигналов как разведки средств связи, так и разведки радиоэлектронных средств.

Полномочия — в данном контексте: права пользователя по доступу к тем или иным ресурсам системы (сети) и на выполнение тех или иных действий в системе (сети). Задаются как правило идентификаторами и паролями. Практикуются различные системы идентификаторов, включая использующие данные биометрии и индивидуальные встраиваемые в личные документы микрочипы.

Пользователь — в данном контексте:
— лицо, использующее в своей служебной или частной деятельности *средства информационные* или *массивы информационные*;
— лицо, обращающееся к информационной системе или посреднику за получением необходимой ему информации и пользующееся ею.

Пользователь уполномоченный — *пользователь*, выступающий в системе или сети как представитель другого пользователя (абонента) и пользующийся его правами (*пользователя полномочиями*) для выполнения каких-либо действий или доступа к информации.

Пользователя полномочия — права *пользователя* по доступу к *системе информационной*, обрабатываемой (хранимой) информации, конкретным техническо-программным средствам или структурам информационной сети.

Потребитель информации — синоним: *пользователь*.

Превосходство информационное — степень доминирования в информационной области, которая разрешает проведение действий без опасности эффективного противодействия.
В военной трактовке: возможность сбора, обработки и распространения непрерывного потока информации, в то же время используя в своих целях или не давая возможности противнику делать то же самое.

Преступление компьютерное — преднамеренная или иная *деятельность неправомочная*, которая воздействует на *пригодность*, *конфиденциальность*, или *целостность* информационных или иных ресурсов с использованием компьютерных средств. *Преступление компьютерное* может включать мошенничество, растрату, воровство,

злонамеренное повреждение, неправомочное использование, отказ или изменение порядка обслуживания и незаконное присвоение.

Преступность информационная международная — использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в противоправных целях.

Пригодность (готовность) информации — обеспечение способности системы продолжать работать эффективно и поддерживать доступность информации. Принцип, который гарантирует, что система и данные работают и доступны пользователям. В этом контексте отказ от обслуживания рассматривается как нападение на пригодность (готовность) информации.

Приемлемый уровень риска — разумная и тщательно рассматриваемая оценка достаточности соответствующей системы защиты минимальным требованиям применяемых директив безопасности. Оценка должна учитывать ценность активов системы, реальные и гипотетические угрозы и практическую уязвимость системы, возможные контрмеры и эксплуатационные требования.

Прикладные ворота — одна из форм *фаэвола*, в которой поступающие данные с прикладного уровня должны быть проверены с целью подтверждения разрешения связи. В случае *ftp* связи прикладные ворота появляются как *ftp* сервер клиенту и как *ftp* клиент к серверу.

Проба — в информационных операциях — любая попытка получения информации об автоматизированных информационных системах или их пользователях, работающих в диалоговом режиме (он-лайн).

Продукт информационный — документированная или переданная по электронным каналам связи информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей.

Проникновение — в данном контексте: успешная *атака* — приобретение способности получить неправомочный и необнаруженный доступ к файлам и программам или системе управления информационной системы (сети). Успешный акт обхода механизмов обеспечения безопасности, неправомочный доступ к информационной системе (сети).

Пропаганда — любая форма распространения информации в поддержку заданных целей, рассчитанная на влияние на мнения, эмоции, отношения или поведение отдельных индивидов или групп, в том числе социальных.

Пространства информационного субъекты — физические и юридические (общественные организации, хозяйствующие субъекты, органы государственной власти) лица, вступающие для реализации своих потребностей или возложенных на них функций во взаимоотношения с использованием *информации* и *инфраструктур информационных*. Являются наиболее важной и системообразующей составляющей *пространства информационного*.

Пространство информационное (инфосфера) — сфера человеческой деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, *инфраструктуру информационно-телекоммуникационную* и собственно *информацию*. Образуется совокупностью субъектов информационного взаимодействия или воздействия; собственно информации, предназначенной для использования субъектами, инфраструктуры, обеспечивающей возможность осуществления обмена информацией между субъектами, общественных отношений, складывающихся в связи с формированием, передачей, распространением, хранением и обменом информацией внутри общества.

Пространство общества информационное — совокупность информации и информационной инфраструктуры, которыми общество располагает или имеет доступ.

Противоборство информационное — 1) форма межгосударственного противоборства, предусматривающая целенаправленное использование специально разработанных средств для воздействия на *ресурс информационный* противостоящей стороны и защиты собственных ресурсов в интересах достижения поставленных политических и военных целей;
2) форма межгосударственного соперничества, реализуемая посредством оказания *воздействия информационного* на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, *инфраструктуру информационную* и СМИ этих государств для достижения выгодных себе целей при одновременной защите от аналогичных действий своего *пространства информационного*.

Противоинформация — действия, направленные на подавление *сферы информационной* противника.

Противоинформация защитная — действия, направленные на защиту своей военной информации от *воздействия информационного* противника.

Противоинформация наступательная — действия, направленные против защитных информационных функций противника.

Противообман — действия, направленные на опровержение, нейтрализацию, принижение влияния или выгоды противника от действия *обмана*. *Противообман* не включает функцию анализа и идентификации действий обмана противника.

Процессы информационные — процессы создания, сбора, анализа, накопления, хранения, поиска, распространения и потребления информации с использованием *инфраструктуры информационной* любого вида или формы. Эти процессы могут быть одиночными или включающими несколько, которые в совокупности составляют более крупную систему или системы процессов.

Прошивка — более точное употребление: «прошивка» устройств ПЗУ. Точно так же, как в программное обеспечение в постоянные запоминающие устройства (ПЗУ) могут быть заложены компоненты, выполняющие непредусмотренные функции. Производители аппаратного обеспечения, прежде всего устройств с постоянными запоминающими устройствами (например, BIOS), могут таким образом внедрять *бомбы логические* или устанавливать *«черные ходы»* в компьютерных системах. Изменения в программное обеспечение различных ПЗУ могут быть внесены и другими лицами, что, например, уже делалось при перепрограммировании модемов. С широким использованием флэш-BIOS процедура внесения таких изменений значительно упростилась и не требует сложного оборудования.

Псевдощель — дополнительная (не скрытая) точка входа, преднамеренно внедренная в операционную систему как западня для *злоумышленников*.

Разработка социальная — 1) термин, используемый в социальной практике для обозначения тактики, используемой при произведении

попыток *доступа неправомочного* к компьютеру (информационной системе), своего рода «catch-all» для выявления возможности получить предназначенный доступ или получить информацию, приближающую к достижению того доступа;
2) нападение, основанное при обмане пользователей или администраторов на целевом участке. Социальные технические нападения типично выполняются, общаясь по телефону с пользователем или оператором и симулируя действия в качестве уполномоченного пользователя, пытаться получать незаконный доступ к системам.

Расплавливание (Ethernet-расплавливание) — форма *атаки*, направленной на перенасыщение Ethernet-узла. Как правило, организуется IP передача, адресованная несуществующему узлу получателя. Это вынуждает маршрутизатор тратить циклы обработки на бесполезный поиск в попытке определить несуществующего получателя и ускорять передачу в ущерб обеспечению нормального движения по сети. Это может являться эффективным средством для *деградации обслуживания* или даже временного *отказа в обслуживании* в данном узле.

Ресурсов информационных владелец — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Ресурсов информационных собственник — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами.

Ресурсы информационные — 1) *инфраструктура информационная*, а также информационные массивы, базы данных и собственно информация и ее потоки.
2) отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других видах информационных систем).

Ретро-вирус — вирус, который не приступает к изменению (разрушению) информации (программ), ожидая, пока все возможные резервные средства восстановления информации не инфицированы настолько, чтобы было не возможно восстановить систему к неинфицированному состоянию.

Рынок информационный — часть общего рынка товаров и услуг. Образуется совокупностью организационных и нормативных механизмов

выявления и удовлетворения потребности физических и юридических лиц в информации по различным аспектам жизнедеятельности человека, общества и государства. В качестве основных элементов *рынка информационного* выступает система организаций, специализирующихся на сборе, обработке и продаже информационных продуктов потребителям.

Сведения критические — сведения, которые требуют непосредственного (немедленного) внимания и реагирования командующего. Включают, но не ограничиваются следующим:
— явные признаки неизбежной вспышки военных действий любого типа (предупреждение нападения);
— агрессия любого характера (природы) против дружественной страны;
— признаки использования ОМУ;
— существенные признаки в пределах потенциальных вражеских стран, которые могут вести к модификации стратегических планов.

Сведения, составляющие государственную тайну — защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести вред безопасности государства.

Связи безопасность — обеспечение защиты, являющееся результатом всех мер, направленных на недопущение лиц, не имеющих на то разрешения, к ценной информации, которая может быть извлечена при обладании и изучении сообщений систем связи или на введение в заблуждение лиц, не имеющих допуска, в их интерпретировании результатов такого обладания и изучения. Безопасность связи включает в себя обеспечение безопасности закрытой связи, безопасность радиопередач, обеспечение безопасности работы средств связи и электронного оборудования и обеспечение физической безопасности материалов и информации по вопросам безопасности связи.

Обеспечение безопасности закрытой связи — компонент обеспечения безопасности связи, являющийся результатом наличия технически совершенных криптосистем и их правильного использования.

Безопасность радиопередач — компонент обеспечения безопасности связи, являющийся результатом всех мер, направленных на защиту радиопередач от перехвата и использования в других целях, кроме криптоанализа.

Обеспечение безопасности средств связи и электронного оборудования — компонент обеспечения безопасности связи,

являющийся результатом всех мер, предпринимаемых, чтобы не допустить лиц, не имеющих на то разрешения, к ценной информации, которая может быть извлечена из перехвата и анализа излучений шифровального оборудования и систем дальней связи.

Физическая безопасность связи — компонент обеспечения безопасности связи, являющийся результатом всех физических мер, необходимых для защиты секретного оборудования, материалов и документов от доступа к ним или наблюдения за ними со стороны лиц, не имеющих на то разрешение.

Связи сети — совокупность электрических сетей связи и сетей почтовой связи. Они функционируют как взаимоувязанный производственно-хозяйственный комплекс, предназначенный для удовлетворения нужд граждан, органов государственной власти и управления, обороны, безопасности, охраны правопорядка, физических и юридических лиц в услугах электрической и почтовой связи.

Связи электрической сети — сети передачи и приема любых знаков, сигналов, текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам. Системы передачи данных являются разновидностью систем электрической связи, в которых передача информации осуществляется в цифровом виде и на основе специальных протоколов обмена информацией между отправителем и получателем.

Связь почтовая — единая технологическая сеть учреждений и транспортных средств, обеспечивающих прием, обработку, перевозку и доставку почтовых отправлений (письма и почтовые карточки, бандероли, пакеты, посылки, почтовые контейнеры, печатные издания в соответствующей упаковке), перевод денежных средств, а также организацию экспедирования, доставки и распространения периодической печати, денежных выплат целевого назначения.

Связь с общественностью — меры по распространению общественной и политической информации и мероприятия по связи с гражданскими органами и населением, направленные на общественность как вне, так и внутри страны.

Секретности информации обеспечение — охрана и защита *информации* и *систем информационных* от несанкционированного доступа или от изменения информации во время ее хранения, обработки или передачи, а

также против воспрещения обслуживания имеющих допуск пользователей. Обеспечение секретности информации включает меры, необходимые для обнаружения, документирования и противодействия таким угрозам. Обеспечение секретности информации состоит из *безопасности компьютерной* и *связи безопасности*.

Синие коробки — устройства, созданные *кракерами* и телефонными *хакерами* — *фрикерами*, чтобы ворваться в телефонную систему и через нее сделать запросы, в обход нормального средства управления и/или процедур контроля доступа.

Система информационная — 1) полная инфраструктура, организация, персонал и компоненты, которые участвуют в сборе, обработке (изменении, обновлении), хранении, передаче, демонстрации и распространении информации;
2) организационно упорядоченная совокупность документов и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Система информационно-телекоммуникационная — совокупность информационно-вычислительных систем, объединенных системой передачи данных. Информационно-вычислительные системы реализуют функции автоматизации процессов сбора, обработки и хранения информации, а системы передачи данных позволяют осуществлять обмен этой информацией между информационно-вычислительными системами, а также обеспечивать доступ удаленных пользователей к хранящейся и обрабатываемой информации.

Спам — метод *кибератаки* — принудительное направление больших количеств, как правило, бессмысленной информации в один или несколько связанных адресов сети. Цель достигается переполнением входных буферов объектов нападения и тем самым фактическое выведение их из строя, когда они будут вынуждены отказывать в обслуживании другим пользователям. Метод особенно применим к узловым серверам больших сетей. В этом случае из строя выходит фактически целая подсеть.

Спуфинг — обобщенный термин, относящийся к методам *проникновения* (*доступа несанкционированного*) в информационные массивы или сети за счет симуляции полномочного пользователя или совершение каких-либо

операций в информационных сетях с неправомерным использованием полномочий или идентифицирующих признаков законного пользователя.

Спуфинг сетевой — получение доступа к ресурсам сети путем обмана, прикрываясь другим адресом: ситуация, когда пользователь пытается соединиться с сервером интернет, proxy-сервером или брандмауэром, используя ложный IP-адрес.

Среда информационная — совокупность отдельных лиц, организаций или систем, занимающихся сбором, обработкой и распространением информации; также сюда включается сама информация.

Средства информации психологические — информационные средства (технические или не технические), которые устанавливают любой вид связи с потенциальными клиентами, используя психологические методы или психологические особенности клиента.

Средства информационные — технико-программные и телекоммуникационные средства, используемые в *процессах информационных*.

Средства передачи данных технические — сети связи и устройства, используемые в процессе передачи информации.

Средства психотронные — специальные технические (генераторы излучений), информационные (видеография и телевизионная информация), химические и прочие средства, предназначенные для дистанционного воздействия на население и группы людей с целью вызвать психические и психофизические изменения (краткосрочного или долговременного характера).

Средства психотропные — специально структурированные лекарства, психофармакологические и психодислептические препараты, транквилизаторы, антидепрессанты, галлюциногены, наркотики, алкогольные компоненты и т.п. средства, предназначенные для воздействия на психику отдельного человека или компактной группы людей.

Структуры критически важные — 1) элементы политико-экономической структуры государства, дестабилизация или блокирование деятельности которых катастрофически скажется на функционировании государства в целом;

2) объекты, системы и институты государства, целенаправленное воздействие на *ресурсы информационные* которых может иметь последствия, прямо затрагивающие национальную безопасность (транспорт, энергоснабжение, кредитно-финансовая сфера, связь, органы государственного управления, система обороны, правоохранительные органы, стратегические информационные ресурсы, научные объекты и научно-технические разработки, объекты повышенной технической и экологической опасности, органы ликвидации последствий стихийных бедствий и иных чрезвычайных ситуаций).

Суверенитет интеллектуальный — право субъекта распоряжаться собственным интеллектом, развивать его, реализовывать его возможности, добывать знания и самостоятельно оценивать поступающую информацию не в ущерб другим субъектам.

Сфера информационная — синоним: *пространство информационное*.

Сфера информационно-психологическая — часть информационной сферы, связанная с воздействием *информации* на психическую деятельность человека. Она образуется совокупностью людей, *информацией*, которой они обмениваются и которую воспринимают, общественных отношений, возникающих в связи с информационным обменом и информационными воздействиями на психику человека.

Телекоммуникации средства — совокупность средств связи, обеспечивающих передачу данных между ЭВМ и информационными системами, удаленными друг от друга на значительные расстояния.

Терроризм информационный — 1) использование информационных средств в террористических целях — угрозы применения или применения физического насилия в политических целях, запугивания и дестабилизации общества, и таким образом оказания влияния на население или государство;
2) действия по дезорганизации автоматизированных информационных систем, создающие опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если они совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях.

В узко правовом смысле информационный терроризм может трактоваться как намеренное злоупотребление средствами информационной системы, информационной сети или их компонентом в целях поддержания или способствования террористической деятельности или отдельному такому действию. В этом случае злоупотребление системой (сетью) не обязательно приводит к прямому насилию против людей, но может быть причиной катастроф или диверсий, в результате которых могут быть человеческие жертвы.

Терроризм информационный международный — использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в террористических целях.

Технология информационная — 1) упорядоченная совокупность процессов и действий по созданию *ресурса информационного*;
2) упорядоченная совокупность процессов и действий, в которых для достижения поставленных целей в качестве основных средств и инструментария используются *средства информационные*;
3) организованная совокупность процессов, элементов, устройств и методов, используемых для обработки информации.

Точность информации — термин используется для характеристики того, что информация поддержана и передана таким способом, что не могла измениться ни злонамеренно, ни случайно. Точность гарантирует против подделки или вмешательства. Нередко трактуется как синоним *целостности*.

«Троянский конь» — 1) независимая программа, исполняющая оговоренные в системе функции, но за счет содержащегося в ней сокрытого куска также производит и неправомерные действия в системе в соответствии с заложенным в этот кусок заданием, часто выступая от имени и с правами пользователя и приводя к фальсификации или разрушению данных;
2) фрагмент компьютерного кода, скрытый внутри инфицированной программы.

Является широко используемым механизмом маскировки проникновения *вирусов* или *«червей»* в систему. Могут маскироваться, в частности, под служебные программы, поставляемые с коммерческими и иными программными комплексами обеспечения безопасности компьютерных систем.

Угроза пассивная — угроза неправомочного раскрытия информации без того, чтобы изменять состояние системы. Тип угрозы, которая подразумевает только перехват, но не изменение или уничтожение информации.

Услуг информационных индустрия — сектор экономики, связанный с производством информационных продуктов, т.е. информации, представленной в виде товара. Этот сектор включает в себя прежде всего информационные агентства, которые профессионально занимаются производством информации для продажи.

Услуги информационные — действия субъектов (*собственников* и *владельцев*) по обеспечению *пользователей продуктами информационными*.

Уязвимости анализ — в *операциях информационных* — систематические проверки *системы информационной* или ее продукции для определения адекватности мер обеспечения безопасности, выяснения дефектов системы мер безопасности, получения данных, позволяющих предсказать эффективность предполагаемых мер безопасности и подтвердить адекватность таких мер после выполнения.

Уязвимость — в данном контексте: известный или подозреваемый недостаток в аппаратных средствах, программном обеспечении или функционировании *системы информационной* (сети), который подвергает систему опасности *проникновения*, а циркулирующую в ней информацию случайному раскрытию. Слабость автоматизированных процедур безопасности системы, административных средств управления, физического расположения, внутреннего управления, и т.д., которая чревата угрозой получения *злоумышленником* неправомерного доступа к информации или случайным прерыванием процессов обработки с искажением или уничтожением информации.

В *операциях информационных* — слабость в проекте, методиках, выполнении и внутреннем контроле безопасности информационной системы, которые могут быть использованы для получения *доступа несанкционированного* к *информации* или *системе информационной*.

Фаэвол — метафорическое название типа аппаратных средств ЭВМ и ресурсов системы защиты компонентов программного обеспечения (например, серверов) от *нападения* через сеть (например, от пользователей интернета) за счет перехвата и проверки поступающей информации сети.

Соединение аппаратных средств ЭВМ и программного обеспечения, выполняющего фаэвол-действия может изменяться в зависимости от доминирующих целей защиты и конфигурации защищаемых систем. Система или комбинация систем, которая предписывает границу между двумя или больше сетями. Ворота, которые ограничивают доступ между сетями в соответствии с «местной» политикой безопасности.

Фаэвол-машина — определенный компьютер, предназначенный для осуществления фаэвол-защиты.

Фишбол — тактика обороны от кибератак, в которой подозрительному или неправомочному пользователю разрешают продолжить установленный доступ к защищенной системе (сети), но ограничивают взаимодействием только с частью системы (сети) в пределах безопасной области его возможных действий (например, направляют по неправильному адресу на изолированный компьютер; переадресуют к фиктивной окружающей среде, моделирующей фактический сервер) так, чтобы сотрудники службы безопасности могли наблюдать и анализировать намерения атакующего, его тактику, и/или пытаться идентифицировать его. Таким образом, целью этой тактики является содержать, изолировать и контролировать неправомочного пользователя в пределах системы, чтобы получать информацию о нем самом.

Фонд информационный — совокупность информационных и интеллектуальных ресурсов, относящихся к целям и интересам их обладателя.

Фракер — *злоумышленник*, комбинирующий хакерские действия и *фрик телефонный*.

Фрик телефонный — вторжение в телефонные системы и системы коммуникаций. Акт использования технологии для нападения на общественную телефонную систему. «Искусство» взламывания телефонной сети. Однако фрик — угроза не только телефонным системам, но и компьютерным сетям и любым системам, использующим телефонные каналы связи.

Фрикер — разновидность *хакера*. Имеет большинство характеристик хакера, по отношению к взлому телефонных систем.

Функция информационная — любая деятельность, предусматривающая приобретение, передачу, хранение или преобразование информации.

Хакер — обобщенное название *злоумышленника*, намеренно находящего доступ к компьютерам и информационным системам, к которым он не допущен. Хакерские действия не обязательно связаны с нарушением информации, но всегда с незаконным проникновением в закрытые информационные системы и сети.

Целостность (информации) — неизменность и неразделимость информации при ее хранении и передаче внутри системы или сети.

Часовая мина — *бомба логическая*, программная компонента, активизация которой производится в определенный временной момент, например, в соответствии с установленной датой и временем. Может рассматриваться как вариант *«троянского коня»*, в котором заложена активизация по временному условию.

«Червь» программный — программа или выполнимый модуль, который способен к самостоятельной активной деятельности, воспроизведению и распространению в распределенных системах или сетях. «Червь» программный может копировать себя, если необходимо, чтобы распространиться на все необходимые ему для собственной обработки ресурсы системы. Такими ресурсами могут быть CPU времени, каналы ввода-вывода или памяти системы. *«Червь» программный* будет копировать себя с машины на машину с использованием связей, установленных внутри сети, часто забивая сети и компьютерные системы. Чтобы копировать себя, *«червь»* должен породить процесс; это подразумевает то, чтобы активно существовать, *«черви»* требуют мультиуправления задачами.

В отличие от компьютерных вирусов, *«червь»* представляет собой самостоятельный программный пакет, предназначенный для самораспространения путем копирования своего пакета с одного компьютера на другой, как правило, через сеть, в том числе и интернет. Другое важное отличие *«червя»* от вируса состоит в том, что он не модифицирует программы компьютерной системы и не повреждает данные на локальном компьютере, а позволяет в соответствии со своим предназначением нарушать работоспособность сети или получать доступ к информационным ресурсам сети, подвергшейся *атаке*.

«Червь» сети — *«червь» программный*, который мигрирует по сети, копируя себя от одной системы к другой, эксплуатируя общие средства обслуживания сети, заканчиваясь выполнением (копированием) *«червя»* в новой системе. Позволяет в соответствии со своим предназначением

нарушать работоспособность сети или получать доступ к информационным ресурсам сети, подвергшейся *атаке*.

Черный ход — специальный программный механизм, действующий в обход систем безопасности и встраиваемый в систему производителем программного обеспечения с целью получения доступа производителя (или лица, чьи интересы он обеспечивает) к информационным ресурсам и настройкам системы. Синонимы: *люк*, *задняя дверь*.

Чехарда (Leapfrog-нападение) — 1) любая форма вторжения (нападения), выполненного через по крайней мере одну-другую промежуточную систему;
2) нелегальное использование идентифицирующих признаков третьего законного пользователя (или итерационно нескольких пользователей) для сокрытия следов незаконного проникновения в сеть (систему).

Шторм почтовый — род *атаки*. Целевая акция инспирирования непомерно большого потока почтовых e-mail сообщений, достаточного для полного прерывания нормальных действий машины или сервера адресата.

ПРИЛОЖЕНИЕ 2. ИНФОРМАЦИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ФИЛОСОФСКИЕ АСПЕКТЫ)

Феномен информации

К началу XXI века в большинстве стран уже осознано то обстоятельство, что в основе функционирования общества и деятельности людей лежат процессы накопления, переработки, передачи и использования информации. Если в 70-е годы концепции информационного общества воспринимались главным образом как футурологические построения, то сегодня задачи формирования такого типа обществ официально провозглашены в качестве приоритетных многими государствами и межгосударственными объединениями, в том числе весьма влиятельными в политическом, экономическом и культурном отношении. «Информационное общество», «информационная экономика», «информационная безопасность», «информационная война» — эти и подобные им выражения больше не являются достоянием лишь узкого круга специалистов, но широко и активно используются в осмыслении разнообразных социальных взаимодействий, содержание и результаты которых невозможно адекватно оценить без понимания самого феномена информации.

Термин «информация» происходит от латинского слова «informatio» — осведомление, изложение, разъяснение. В повседневном сознании этому термину соответствовало представление об информации как о сообщениях, сведениях, имеющих определенное содержание. Толковые словари особо выделяли понимание информации как данных, новостей, сведений и знаний, полученных путем исследования и наблюдения, а также как фактов, приготовленных для сообщения.

Попытки научного исследования феномена информации предпринимались в рамках теории журналистики еще в 20-30-х годах XX века.

Однако темой «земных» научных дискуссий феномен информации стал лишь во второй половине столетия. И произошло это благодаря появлению теоретических построений, стимулированных не проблемами журналистики, а потребностями техники связи и создания вычислительных машин, в том числе для военных целей.

Формированию «информационного взгляда» на привычные и вновь конструируемые объекты в большой степени способствовала деятельность Н. Винера, который рассматривал понятие информации как

одно из основных понятий кибернетики — «теории управления и связи в машинах и живых организмах».

Все более широкое осознание социальной значимости информации в течение второй половины ушедшего столетия было обусловлено техническими, экономическими, политическими, военными и культурными факторами. Среди них — возникновение и интенсивное развитие электронно-вычислительной техники, вскоре конвергировавшей с телекоммуникационной техникой, усложнение технических, экономических и социальных структур и, соответственно, процессов переработки информации, требуемой для функционирования этих структур, трудности управления большими системами в различных сферах, возрастание объемов и общественного значения различных видов социальной информации, от научно-технической до массовой, формирование информационной индустрии, охватывающей такие, традиционно считавшиеся отдаленными друг от друга, отрасли, как производство электроники и выпуск кинофильмов. Появление и широкое распространение персональных компьютеров, доступных непрофессиональному пользователю, создание открытых компьютерных сетей и, в первую очередь, интернета, ставшего информационно-технологическим символом современной эпохи, способствовали повышению общественного внимания к вопросам производства и использования информации, к проблемам информационной политики и стратегии.

На этом фоне закономерным выглядит широкое распространение социально-политических идей, связанных с понятием информационного общества. В конце 60-х — начале 70-х годов в Японии была разработана концепция информационного общества, предполагавшая повышение «информационной емкости» продуктов производства за счет увеличения в их стоимости доли инноваций, дизайна и маркетинга, а также превращение производства информационного (не материального) продукта в движущую силу формирования и развития общества[1]. Впоследствии произошла своеобразная конвергенция идей информационного общества с идеями постиндустриализма. В концепции информационного общества, развитой американским социологом Д. Беллом, знание и информация наделяются статусом «стратегического ресурса» и «решающих переменных», заменяющих такие «решающие переменные индустриальной стадии», как труд и капитал[2]. С этими идеями согласуются предлагаемые современными

[1] Masuda Y. The Information Society as Postindustrial Society. Wash., World Future Soc., 1983.

[2] Белл Д. Социальные рамки информационного общества / Гуревич П.С. (ред.). Новая технократическая волна на Западе. М., 1988.

исследователями характеристики информационного общества как «общества, основанного на знании», где обеспечиваются возможности доступа индивидов и групп к информации и знаниям, необходимым для жизнедеятельности и решения личных и социальных задач[3].

В современном обществе информация выступает в различных ипостасях. Это и особого рода ценность-ресурс, которая должна стать доступной как можно большему числу людей, и такая ценность-ресурс, которую следует защищать от нежелательных воздействий и несанкционированного доступа. Информация — средство достижения адекватного понимания целей, задач и содержания деятельности социального субъекта (индивида, организации, государства) другими участниками коммуникативных процессов, условие создания благоприятной обстановки для реализации данных целей, каковые представляются как минимум, правомерными. Вместе с тем информация — средство воздействия на индивидуальное, групповое и общественное сознание, имеющее мощный (преднамеренный или побочный) деструктивный эффект, блокирующее способности подвергающегося воздействию субъекта к продуктивной деятельности, к реализации собственного творческого потенциала, а в предельном случае ведущее к его социальному уничтожению.

Что же такое информация? С одной стороны, расширение сферы использования термина, вовлечение в эту сферу все новых контекстов неизбежно ведет к возрастанию омонимии, когда слову «информация» соответствуют разные смыслы и значения. С другой стороны, особую важность приобретает философское осмысление природы информации, сравнение различных подходов к ее изучению, выявление преимуществ и пределов применимости предлагаемых трактовок.

Понятие информации. Основные трактовки

Большое влияние на определение предметной области понятия информации оказала шенноновская статистическая теория связи. Подход К. Шеннона[4] и его коллег во многом определялся проблемами надежности и безопасности передачи информации, т.е. говоря современным языком информационной безопасности систем связи. Шеннон сформулировал точное понятие количества информации, предположив, что информация — это лишь такие

[3] Ракитов А.И. Философия компьютерной революции. М., Политиздат, 1991; Ершова Т.В. Концептуальные вопросы перехода к информационному обществу. *Вестник РФФИ*, №3, 1988; Мелюхин И.С. Информационное общество. М., Изд-во МГУ, 1999.

[4] Шеннон К. Работы по теории информации и кибернетике.

сведения, которые уменьшают или снимают неопределенность, существовавшую до их получения, и определил количество информации как функцию от вероятности сообщения. «Основная задача связи, — писал Шеннон, — состоит в точном или приближенном воспроизведении в некотором месте сообщения, выбранного для передачи в другом месте. […] Существенно лишь, что посылаемое сообщение является сообщением, выбранным из некоторого множества возможных сообщений».

Хотя вероятностно-статистические трактовки информации получили большую известность и влияние, были предложены и иные подходы к определению количества информации, например алгоритмический подход А.Н. Колмогорова, или термодинамическая интерпретация понятия информации.

Точность и эффективность количественных определений информации достигалась за счет исключения из рассмотрения «человеческого элемента» с его смыслами и целями. Образно говоря, такой подход соответствовал задаче инженера связи — в точности передать знаки, содержащиеся в телеграмме, независимо от ее смысла и ценности для получателя. Развитие техники средств связи принципиально мало что изменило в этом отношении. Надежность и скорость передачи информации вне зависимости от того, что передается — изображения фонтанов Петергофа, порнографические картинки, тексты научных монографий или сообщения о политических скандалах, — определяют качество работы технических средств электронной коммуникации.

Первые логико-семантические трактовки информации определялись не потребностями передачи сообщений по каналам связи, а задачами анализа языка науки с использованием средств математической логики. В известной работе Р. Карнапа и И. Бар-Хиллела[5] информация, содержащаяся в некотором высказывании, эксплицируется как класс логически возможных ситуаций («описаний состояний»), где данное высказывание является ложным. Поскольку в содержательном плане описания состояний представляют собой совокупности суждений о единичных фактах, которые могут наличествовать или отсутствовать в действительности, данная трактовка информативности согласуется с «повседневным» пониманием информации как данных и фактов, противопоставляемых умозрительным спекуляциям. Определение менее вероятного суждения как более информативного соответствует характерным для журналистской практики представлениям об «идеальной» информации как сенсации, сообщении о «невероятном» событии.

[5] Carnap R., Bar-Hillel Y. An Outline of Theory of Semantic Information. Techn. Rep. MIT, 1952.

Впоследствии логики затратили немало усилий на разработку более утонченных интерпретаций информации, учитывающих познавательные возможности субъекта и особенности ситуаций решения проблем, позволяющих определять информативность логических процедур[6]. Это относится и к тем вариантам логико-семантического анализа, которые рассматривают информацию в коммуникативном контексте. Примером может служить предложенная Ю.А. Шрейдером трактовка информации в рамках модели коммуникации, согласно которой количество семантической информации, содержащейся в сообщении, есть характеристика изменений в языке участника, а следовательно, в сознании коммутанта.

Прагматические концепции информации стремятся в возможно большей мере учесть ее «человеческие» аспекты, принимая во внимание цели, прогнозы и планы действий субъекта. Здесь используются такие понятия, как ценность и польза информации для ее обладателя. Например, А.А. Харкевич связывал ценность с использованием информации для определенной цели. «Информация, — писал он, — ценна, поскольку она способствует достижению поставленной цели. Одна и та же информация может иметь различную ценность, если рассматривать ее с точки зрения использования для различных целей. Так, сообщение о погоде имеет значительную ценность для охотника, но не представляет обычно никакого интереса для игрока в карты»[7]. Согласно М. Бонгарду, мера полезной информации имеет тем большую величину, чем меньше предполагаемое наблюдателем распределение вероятностей («гипотеза наблюдателя») отличается от действительного распределения вероятностей.

В 70-е годы А.Д. Урсул и Б.В. Бирюков, отталкиваясь от концепции разнообразия У. Эшби, опиравшейся на статистическую теорию информации, предложили более широкий взгляд на информацию. Информация понимается ими как отраженное разнообразие, а информационный процесс — как отражение разнообразия[8]. Практически не касаясь вопроса о канале связи, по которому передается информация, эти авторы сосредоточили внимание на объекте-носителе передаваемого разнообразия («отражаемый объект») и объекте, которому передается разнообразие («отражающий объект», получающий, воспринимающий, «усваивающий» разнообразие). Эта трактовка информации, развиваемая

[6] Войшвилло У.К. Семантическая информация. Понятия экзистенциональной и интенсиональной информации / Кибернетика и современное научное познание. М., 1976; Хинтикка Я. Логико-эпистомологические исследования. М., 1980; Брюшинкин В.Н. Логика, мышление, информация. Л., Изд-во ЛГУ, 1988.

[7] Харкевич А.А. О ценности информации. Проблемы Кибернетики, Вып.4, 1960.

[8] Берга А.И. и др. (ред.). Управление. Информация. Интеллект. М., Мысль, 1976.

также и другими авторами[9], в какой-то мере согласуется с общежитейскими представлениями об информации как о сведениях, отражающих разнообразие. Она не вступает в явное противоречие с имеющимися концепциями информации и допускает определенные аналогии с ними. Понятие отражения в данном случае выводится за пределы теории познания и выступает как онтологическая категория. Приверженцы данного подхода видели одно из основных его достоинств в том, что он открывал возможности для «охвата» информации в природных системах.

Общефилософские концепции информации (и это признают их авторы) далеки от того, чтобы «охватить» все имеющиеся научные трактовки информации и представить их в качестве конкретизаций «философского понятия» информации. Данные концепции являются лишь результатом интерпретации феномена информации средствами одной из областей знания - в данном случае философии.

Из факта отсутствия общей дефиниции информации, под которую можно было бы подвести все другие ее трактовки как частные, вовсе не следует, что различные концепции информации не имеют между собой ничего общего. Подобный вывод был бы неверным уже в силу того, что идеи, характерные для одних концепций и подходов, так или иначе преломляются в других концепциях и подходах.

Традиция обсуждения проблем природы информации приобретает новую актуальность сегодня, когда расхождения в понимании того, что такое информация, могут стать препятствием к взаимопониманию при разработке международных соглашений, направленных на обеспечение информационной безопасности. Следует подчеркнуть, что для российской традиции (неотъемлемым компонентом которой всегда был живой интерес к зарубежным концепциям и подходам) характерен широкий взгляд на феномен информации, связывающий информацию с явлениями любой природы и охватывающий ее материальные, технологические, логико-лингвистические, социальные и гуманитарные аспекты.

Информация как основа социальной коммуникации

В многообразии видов информации мы выделяем те, которые составляют основу социальной коммуникативности, т.е. относятся к социальной

[9] Ракитов А.И. Философия компьютерной революции.

информации. Под социальной информацией в широком смысле этого слова понимается информация, получаемая и используемая людьми в различных сферах деятельности.

К основным видам информационной деятельности относятся[10]:

- производство информации (представляющее собой закрепление тех или иных результатов познавательной деятельности человека в системах знаков);
- перенесение смыслового содержания из одной семиотической системы в другую (перевод информации);
- воспроизведение одного и того же информационного продукта в большем или меньшем количестве экземпляров (тиражирование информации);
- передача (трансляция или ретрансляция) информации с помощью или без помощи технических средств;
- использование информации для создания новой информации или для достижения иных эффектов;
- хранение информации, понимаемое как обеспечение возможности ее актуализации во времени, включающей передачу и потребление;
- разрушение информации путем физического разрушения материальной основы знаков или морального уничтожения (дезавуирования) текста, создание технических или семиотических препятствий передаче информации.

Другие виды информационной деятельности могут рассматриваться как сочетания перечисленных видов, рассматриваемых как базовые. Например, распространение информации предполагает ее передачу и тиражирование, которые могут осуществляться практически одновременно.

Сохранение и развитие социума зависит от результатов информационной деятельности субъектов, представляющих различные имеющиеся в нем группы и сегменты. Инженер, управляющий системами жизнеобеспечения города, работник навигационной службы, ученый (естественник или гуманитарий), производитель товаров и услуг и их потребитель, журналист и обыватель, писатель и государственный чиновник так или иначе вовлечены в процессы производства, перевода, передачи информации, а также в другие виды информационной деятельности, вынуждены (осознанно или нет — особый вопрос) принимать, выбирать или разрабатывать определенные коммуникативные стратегии.

[10]Проводимое здесь различение видов информационной деятельности основывается на типологизации, представленной в работах Б.А.Грушина.

В коммуникативных стратегиях неизбежно присутствует информационное взаимодействие. Именно на этом базируется анализ процесса коммуникации, учитывающий изменения в «инфофондах» (информационных фондах) всех его участников[11]. Это изменения в знаниях субъекта об окружающей действительности и о себе самом, в языке, воплощающем эти знания, в способностях коммуниканта воспринимать и аккумулировать сообщения.

Коммуникация крупных социумов, каковыми являются национальные общества, формально является равноправной. Однако порождаемые ею изменения в инфофондах участников значительно различаются по характеру, глубине и интенсивности. Перенесение правил, установок и ценностей (информационное воздействие), выполняющих организующую роль в инфофонде одного, более «сильного» социума, в другой, более «слабый», при определенных обстоятельствах может привести к дезорганизации последнего. К таким обстоятельствам относится отсутствие адекватных механизмов интерпретации и условий реализации соответствующих установок, наличие в «принимающем» инфофонде блокирующих императивов и т.д.

Техноцентристским идеалом глобального информационного общества является совершенствование информационных технологий, их распространение по всему миру и расширение доступа к информационным ресурсам. Предельным случаем выступает ситуация, когда любой человек, находящийся в любой точке земного шара (и даже за его пределами), в любой момент времени может получить необходимую ему информацию. Собственно, этот идеал и задает магистральное направление в движении к информационному обществу, а затем в совершенствовании такого общества и достижении им стадии зрелости. В подобном контексте информация видится как некая субстанция, которой одновременно может пользоваться сколь угодно большое число людей без всякого ущерба для нее самой, а развитие демократии рассматривается как направленное на обеспечение технических и организационных возможностей для доступа к такой ценной вещи, как информация.

Так, формирование сознания современного человека становится объектом (и результатом) конкурентной борьбы на рынках аудиовизуальной продукции, создатели которой, как правило, исходят из соображений выгоды, далеко не всегда согласующихся с гуманистическими идеалами,

[11]Термин «инфофонд» мы используем вслед за В.З. Коганом. См.: Коган В.З. Человек в потоке информации. Новосибирск, Наука, 1981.

а проблема выбора информационных продуктов и услуг представляет непростую задачу для потребителя.

В современных условиях решающее значение приобретает ответственное отношение социального субъекта к собственному инфофонду и к возможным последствиям своей деятельности для инфофондов тех субъектов, которые она так или иначе затрагивает. Формированию такого рода ответственного отношения может способствовать осознание проблемы интеллектуального суверенитета. Вид суверенитета зависит от того, какие права принимаются во внимание. Когда речь идет о правах познавательных, мы имеем дело с интеллектуальным суверенитетом.

Очевидно, что не существует и никогда не существовало интеллектуального суверенитета в чистом виде. Всегда есть границы, обусловленные принятием на веру мнений других людей, усвоением результатов их интеллектуальной деятельности. Эти границы, конечно же, не являются четкими. Однако в случае угрозы сужения привычных пределов (действительной или мнимой) возникает напряжение, побуждающее к осознанию значимости наших интеллектуальных возможностей и прав.

Примечательно, что современные сетевые коммуникации создают вызовы суверенитетам всех национальных государств и не только отстающих в информационно-технологической гонке. Данная ситуация служит подтверждением актуальности выделения и изучения специфических видов суверенитета, значимость которых осознается именно в условиях развития современных информационных технологий. Кроме того, следует иметь в виду, что политический суверенитет государства и интеллектуальный суверенитет нации могут находиться в весьма непростых отношениях[12].

Реализация интеллектуального суверенитета не сводится к охране инфофонда от негативных воздействий извне. Необходимы не только защита информации, а и адекватная ее квалификация, аналитическое отношение к синкретическим информационным воздействиям. При этих условиях средства защиты информации играют важную роль, обеспечивая условия для обогащения и обновления инфофонда социальных субъектов за счет надежных данных, концептуальных структур и ценностных ориентиров, необходимых для эффективной организации опыта, адекватной постановки и решения задач. Все это предполагает как творческую деятельность субъекта в сфере собственного «информационного производства», так и активное участие во «внешних» процессах социальной коммуникации.

[12]Weckert J. What is New or Unique about Internet Activities. Macmillan, Internet Ethics, 2000.

Изложенные выше соображения могут служить концептуальными предпосылками многоаспектного анализа проблематики информационной безопасности.

Сетевая информационная революция

Сегодня стало очевидным преобладание информационной составляющей деятельности людей над всеми ее другими формами и компонентами. Именно поэтому современные информационные технологии являются подлинным локомотивом мирового экономического и технологического развития.

Мультипликативный эффект открытий и изобретений в области обработки информации и коммуникации проявляется неотвратимо. История дает нам несколько примеров этих эффектов, которые с полным основанием можно называть информационными революциями[13]. Каждый информационно-технологический прорыв проявляется во все более глобальном масштабе. Именно новые информационные и телекоммуникационные технологии несут в себе огромный потенциал повышения производительности труда, производства усовершенствованных товаров и услуг, реального повышения качества жизни. Они составляют не только фундамент каждого нового технологического уклада, но и представляют главную движущую силу смены укладов, изменяющей облик цивилизации.

Пожалуй, первым технологическим достижением, имевшим огромное общественное и культурное значение, было изобретение И. Гутенбергом печатного станка, использовавшем подвижные металлические литеры. Библия Гутенберга, напечатанная в 1456 г., приоткрыла дверь в культурное пространство, передвижение в котором привело нас через 500 лет в информационный век. Впервые в истории человечество получило возможность массово производить и распространять информацию. Впервые знания, мнения и опыт оказалось возможным передавать в компактной, сохраняемой длительное время и общедоступной форме. Доступность информации массам превратилась в течение веков в грозное политическое и экономическое оружие. Великие книги, хартии и декларации, манифесты и конституции — все они дали начало политическим, национальным и религиозным идеям, убеждениям и принципам, составляющим духовную сокровищницу современного человечества[14].

[13]Смолян Г.Л., Черешкин Д.С. Пятая информационная революция. *Мир связи. Connect*, No. 7-8, 1997.
[14]Boorstein D. The Discovers. N-Y., Random House, 1983.

Вторым технологическим изобретением, революционно изменившим способ обмена информацией, был телефон. Аппарат А. Белла, запатентованный им 10 марта 1876 г., оказался первой сугубо личной коммуникационной технологией. Немногим более чем за десятилетие телефонные станции с электромеханическим селектором номеров получили широкое распространение и к 1904 г. телефонная система оплела значительную часть американского континента. Сегодня сотни миллионов людей общаются посредством каналов проводной, оптоволоконной или радиотелефонной связи и электронных АТС когда хотят, с кем хотят и как хотят, образуя пространство личных информационных обменов.

Третью революцию в обмене информацией совершило радио, предоставившее эффективный и удобный способ связи без проводов. Г. Герц, Н. Тесла, Г. Маркони и А. Попов — все они, первооткрыватели радио, обессмертили свои имена. А через шесть десятилетий спутниковая радиосвязь преобразовала межконтинентальный информационный обмен. Она кардинально расширила понятие коммуникационной сети, телефонной системы и информационного пространства.

Четвертую информационную революцию совершил персональный компьютер. Если вторая и третья революции охватывали средства передачи информации, то создание персонального компьютера решительно преобразовало способ формирования, организации и распространения знания. Это изобретение позволило массе людей приобщиться к профессиональным знаниям, общественному информационному богатству без помощи посредников и тем самым превратить профессиональные знания в личностно-значимые. Интеллект человека, поддерживаемый персональным компьютером, стал инструментом, ориентированным на самопознание и саморазвитие[15]. Персональный компьютер — это конструктор интеллектуального действия, он превращает человека, говоря словами М.М. Бахтина, в автора и героя этого действия, в его режиссера и зрителя. Персональная компьютерная вездесущность широко распахнула ворота в информационный век, узкая щель в который была приоткрыта, как мы видели, в XV веке.

Теперь осталось лишь обеспечить легкий и свободный доступ к информации по всему миру. Это и происходит сегодня, причем революционное значение сетевых коммуникационных технологий уже осознано одновременно с их

[15]Смолян Г.Л., Шошников К.Б. Феномен персональной ЭВМ — философско-методологический аспект. *Вопросы Философии*, №6, 1986.

созданием. Глобальная информационная инфраструктура, информационная супермагистраль, — это различные наименования пятой информационной революции, революции в телекоммуникациях. Эти метафоры означают, что новые технологии уничтожают понятие расстояния как таковое.

Фактически эта революция интегрирует эффекты всех предшествующих, ибо создает технологическую основу объединения интеллектуальных способностей и духовных сил всего человечества. Как никакое предшествующее открытие или изобретение в мире информации и коммуникаций, сетевая информационная революция оказывает мощное воздействие на все сферы жизни общества: политику, экономику, культуру.

Видимо, первой особенностью сетевого взаимодействия можно назвать очень высокую, практически мгновенную скорость циркуляции информации. Второе, это предоставление невиданных ранее возможностей доступа профессиональных и непрофессиональных абонентов сетей к мировым информационным ресурсам. При этом стираются отличия между локальными и распределенными хранилищами информации, а сама сеть становится глобальным хранилищем. Нужные пользователю данные организованы в удобные страницы, так что ему остается только листать книгу, вместо того, чтобы перебирать файлы на дискетах.

Именно опыт развития мировых открытых сетей, например интернета, позволяет говорить о начале новой эры в развитии средств и систем переработки информации. При этом под переработкой понимается вся совокупность выполняемых при этом процессов — сбор, обработка, хранение, накопление, представление, передача и защита информации. В таких сетях пользователь воспринимает сам себя и воспринимается другими как неотъемлемый компонент единого информационного сообщества. Компьютерные и телекоммуникационные сети наших дней — явление глобального масштаба. Без особого преувеличения можно говорить, что они способны перелицевать политическую карту мира и изменить сложившиеся отношения между геополитическими центрами силы. Практически для всех стран мира они ставят по меньшей мере три класса непростых проблем:

- во-первых, необходимо понять, как надо строить межгосударственные отношения в новых условиях информационной проницаемости государственных границ;
- во-вторых, надо выбирать рациональную политику по отношению к глобальной сети и вхождению национальных телекоммуникационных сетей в них;

- в-третьих, надо думать о том, как предотвращать угрозы использования новых информационных технологий в качестве информационного оружия.

Глобальные сети, конечно, мощное средство информационного объединения стран и народов, предпосылка их экономической и политической интеграции. Информационно-технологические достижения оказались завязанными с политическими решениями в единую цепочку. Трансграничный информационный обмен в областях науки, техники, образовательных программ, искусства, развлечений и, наконец, массовой коммерческой и бытовой жизни, становится всеохватным, во многом способствующим превращению государственных границ в условные разделительные линии. Нельзя не признать, что интегративные процессы в Европе в большой степени обязаны быстрым развитием интернета.

Представляется вполне очевидным, что мировые открытые сети могут оказаться инструментом информационной, политической и культурной экспансии информационно-технологически развитых стран по отношению к неразвитым или развивающимся. Появились новые реальности межгосударственных отношений, новая расстановка сил на мировой арене, когда во внешнеполитическую ткань вплетаются интересы информационного доминирования одних стран над другими. Надо отдавать себе отчет, что когда «переход» информации через границу практически не контролируется, возникают проблемы (сохранение конфиденциальности информации, определение ее стоимости и т.д.), могущие существенно осложнить межгосударственные отношения. Это проблемы общие для всех стран, вне зависимости от уровня их технологического развития.

Как правило, отстающие и развивающиеся страны не имеют достаточно средств и производственных возможностей для самостоятельного создания и развития национальных телекоммуникационных сетей и вынуждены привлекать для этого капиталы, технику и технологии развитых стран, что и делает возможным попадание таких стран в политическую зависимость.

Серьезное геополитическое значение имеют угрозы использования новых информационных технологий в качестве информационного оружия. Сегодня это понятие быстрыми темпами переходит из научной фантастики в область реальной жизни. Примеров разрушения информационных ресурсов и телекоммуникаций, несанкционированного доступа к ним, модификации значимой информации и тому подобных

действий множество. Они совершались во все времена, но только сегодня они стали приобретать глобальный политически значимый характер.

Большую опасность представляют сегодня возможности информационно-террористических действий, предотвращение которых затруднительно, а нейтрализация последствий безумно дорога. Это определяет необходимость международных усилий, разработки международных соглашений по запрещению или ограничению возможностей использования информационного оружия по типу международных соглашений по ограничению ядерного оружия.

Далее, пятой революцией рожден замечательный парадокс: расширение информационного пространства для межличностного общения не может не считаться социальным благом. И в то же время информационные богатства, выплескиваемые на экраны сетевых компьютеров, навязывают индивиду культурный выбор, зачастую сделанный другими. Технологический синтез компьютерных и телевизионных технологий сети делает открытые сети по силе культурного воздействия сравнимыми со СМИ. Эта тенденция отчетливо проявляется сегодня в увеличении объемов и усилении роли игровой и развлекательной информации, распространяемой по открытым сетям.

Наконец, фактически сформирована сетевая среда глобального манипулирования индивидуальным и общественным сознанием. Эта среда позволяет:

- легко осуществлять оперативное манипулирование общественным мнением, формировать политические установки и портреты политических лидеров;
- широко использовать неосознаваемые информационные воздействия во враждебных или корыстных целях;
- формировать виртуальный мир, подменяющий политическую и экономическую реальность.

Все это не означает, что одни страны должны отмежеваться от других, однако, эти и другие не упомянутые здесь опасности создают платформу для развертывания информационно-психологической борьбы против государств, стран и народов.

Сетевая информационная революция есть еще одно свидетельство того, что технологические достижения человечества могут использоваться в различных целях. Сами машины, как писал Р. Брэдбери, это пустые

перчатки, которые надевает человеческая рука. В актуальном для сегодняшней России политическом контексте это означает, что сетевые технологии ставят трудную и противоречивую задачу перед российским государством. Суть дела в том, что сетевые технологии - мощное средство как децентрализации, так и централизации распространения и использования информации по всей вертикали экономического и политического управления, делающее информационно прозрачной или информационно непроницаемой жизнь управляющей элиты.

Другой аспект. Интерактивные мультимедийные сетевые технологии открывают простор для циркулирования в сети аудиовидеоинформации, распространяющей ненависть, насилие, жестокость, бездуховность. Разумеется, никакие ссылки на свободу слова и информации, на культурное многообразие не могут служить оправданием этому. Равно как и новейшим проявлениям информационного террора, когда в сети легко найти рецепты изготовления наркотиков, взрывчатых и отравляющих веществ. Поэтому так важны усилия по созданию нормативной правовой основы, способствующей, как подчеркивается в проекте резолюции одного из комитетов Совета Европы от 6 января 1997 г., «вкладу новых технологий и новых коммуникационных служб в развитие свободы слова и информации, творческого созидания и обменов между культурами, образования и участия людей в общественной жизни при одновременном решении новых вопросов, возникающих в связи с этими технологиями и службами для защиты прав человека и демократических ценностей».

Информационное неравенство

Информационное неравенство (цифровое неравенство, цифровой разрыв) — это характеристика состояния и уровня развития различных стран, регионов, сообществ и социальных слоев (групп) по критерию вовлеченности их в движение к глобальному информационному обществу[16]. Этот критерий обычно включает: во-первых, оценку доступа к современным информационно-коммуникационным технологиям, информационным системам и сетям и, во-вторых, оценку готовности населения к жизни и работе в информационном обществе. Первая оценка охватывает, преимущественно, степень использования интернета специалистами, чиновниками и населением, уровень развития электронной коммерции, а также реальной обеспеченности конституционного права граждан на доступ к мировым и национальным (государственным) информационным ресурсам

[16]Проблемы преодоления цифрового неравенства. Материалы международного семинара. М., 2000.

в особенности в отсталых городских, сельских и отдаленных районах. Вторая оценка включает в себя социокультурные сдвиги, вызванные распространением информационно-коммуникационных технологий, уровень компьютерной подготовки и осведомленности граждан о возможностях информационно-коммуникационных технологий, степень информационной активности населения и некоторые другие показатели.

Информационное неравенство является следствием неравномерности социально-экономического развития стран, регионов и различных слоев населения и ведет к углублению социально-культурных различий между ними. Оно имеет глубокие причины, коренящиеся в повышении социальной и экономической значимости информации на рубеже веков[17]. Суть дела в следующем.

Во-первых, в результате усложнения общественной жизни увеличиваются информационные потребности людей. Информация превращается в массовый продукт. Растущую потребность в информации начинают испытывать не только управляющая элита, но и миллионы граждан. Это связано с децентрализацией (повышением степени свободы индивидуумов, групп и регионов) современного общества.

Во-вторых, информация как содержание сообщений становится экономической категорией. Она получает рыночную оценку и перестает быть бесплатным товаром. Возникает информационный рынок, где информация продается и покупается, а операции с информацией приносят прибыли и убытки. Расширяются инвестиции в информационную сферу с целью получения новой информации, создания различного рода инноваций для извлечения дополнительной прибыли, а также для воздействия на поведение людей.

В-третьих, в обществе наблюдается неравномерное распределение информации, она не одинаково доступна для различных индивидуумов. Это приводит к тому, что одни индивидуумы получают информационное преимущество перед другими, постепенно трансформируемое в экономическое, социальное или политическое преимущество. Информационное преимущество становится важной социальной силой, способствующей перераспределению экономических, социальных и политических (властных) ресурсов. Иначе говоря, информационное неравенство ведет к социальному неравенству. Верно, конечно, и обратное, однако в наше время первое стало более существенно, чем второе.

[17]Костюк В.Н. Информация как социальный и экономический ресурс. М., 1997.

В-четвертых, эволюция общества становится менее предсказуемой, чем в прошлом. Частично это является следствием усиления воздействия человека на природу, изменяющего природу и тем самым ведущего к изменению среды его обитания; частично это связано с убыстрением темпов эволюции, что побуждает общество и образующие его компоненты быстрее реагировать на происходящие изменения. И то, и другое предполагает значительный сдвиг используемых человеком ресурсов от вещественных к информационным. Можно сказать, что современное общество использует четыре основных ресурса: природные богатства, труд, капитал и информацию (постоянно обновляемые теоретические знания и различного рода сведения, в том числе практические навыки людей). Первые три остаются главными факторами производства, последний — необходимым условием их эффективного использования.

Наличие глобального, регионального и странового информационного неравенства делает проблематику информационной безопасности еще более актуальной, поскольку только обеспечение международной и национальной информационной безопасности может смягчить информационное расслоение стран и тем самым создать условия для их согласованного и устойчивого движения по пути формирования глобального информационного общества.

ПРИЛОЖЕНИЕ 3. ЗАКОНОДАТЕЛЬСТВА ОТДЕЛЬНЫХ СТРАН, ПОСВЯЩЕННЫЕ ПРОБЛЕМЕ НЕЗАКОННОЙ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Борьба с компьютерной преступностью (киберпреступностью) в последнее десятилетие занимает значительное место в законотворческом процессе многих стран. В целях предотвращения ухода преступников от ответственности по национальным законодательствам за счет эмиграции или совершения его с территории других стран предпринимаются попытки нахождения путей гармонизации национальных законодательств и подготовки международно-правовых документов.

Опыт уголовно-правовой классификации преступлений в сфере компьютерной информации, накопленный в ведущих промышленно развитых государствах мира, был обобщен в разработанном государствами-участниками Европейского сообщества и официально оформлен как «Руководство Интерпола по компьютерной преступности», включающем, в частности, «Минимальный список нарушений» и «Необязательный список нарушений».

«Минимальный список нарушений» содержит восемь основных видов компьютерных преступлений:
- компьютерное мошенничество;
- подделка компьютерной информации;
- повреждение данных ЭВМ или программ ЭВМ;
- компьютерный саботаж;
- несанкционированный доступ;
- несанкционированный перехват данных;
- несанкционированное использование защищенных компьютерных программ;
- несанкционированное воспроизведение схем.

«Необязательный список» включает в себя следующие компьютерные преступления:
- изменение данных ЭВМ или программ ЭВМ;
- компьютерный шпионаж;
- неразрешенное использование ЭВМ.

Кроме того, рабочей группой Интерпола был разработан специальный кодификатор, который был положен в основу автоматизированной информационно-поисковой системы, созданной в начале 90-х годов. В

кодификаторе все компьютерные преступления классифицированы следующим образом.
QA — несанкционированный доступ и перехват:
QAH — компьютерная «атака»;
QAI — перехват;
QAT — «кража» времени;
QAZ — прочие виды несанкционированного доступа и перехвата.
QD — изменение компьютерных данных:
QDL — «логическая бомба»;
QDT — «троянский конь»;
QDV — «компьютерный вирус»;
QDW — «компьютерный червь»;
QDZ — прочие виды изменения данных.
QF — компьютерное мошенничество:
QFC — мошенничество с банкоматами;
QFF — компьютерная «подделка»;
QFG — мошенничество с игровыми автоматами;
QFM — манипуляции с программами ввода/вывода;
QFP — мошенничество с платежными средствами;
QFT — телефонное мошенничество;
QFZ — прочие компьютерные мошенничества.
QR — незаконное копирование:
QRG — компьютерные игры;
QRS — прочее программное обеспечение;
QRT — топология полупроводниковых устройств;
QRZ — прочее незаконное копирование.
QS — компьютерный «саботаж»:
QSH — с аппаратным обеспечением;
QSS — с программным обеспечением;
QSZ — прочие виды «саботажа».
QZ — прочие компьютерные преступления:
QZB — с использованием компьютерных досок объявлений;
QZE — хищение информации, составляющей коммерческую тайну;
QZS — передача информации, подлежащая судебному рассмотрению;
QZZ — прочие компьютерные преступления.

Совет Европы совместно с США, Канадой, Японией и ЮАР готовит международный договор, призванный унифицировать законы, связанные с компьютерными преступлениями.

Создаются неофициальные организации, занимающиеся выработкой законодательных актов в борьбе с различными компьютерными преступлениями.

Однако пока определения компьютерных правонарушений и, соответственно, предусмотренные за них наказания различны в разных странах.

Ниже приведены выдержки из национальных законодательств некоторых стран, относящиеся к незаконной деятельности в информационной сфере.

Россия

В России принят ряд законодательных актов, относящихся к компьютерным преступлениям.

В Уголовном кодексе РФ, принятом Государственной Думой 24 мая 1996 г. и одобренном Советом Федерации 5 июня 1996 г. предусматриваются следующие наказания за компьютерные преступления.

Глава 28. Преступления в сфере компьютерной информации.
Статья 272. Неправомерный доступ к компьютерной информации.
1. Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, 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 от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

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 пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, 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 от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти 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.

Деятельность в сфере информации регламентируют и другие законы:
Закон РФ «О средствах массовой информации» (№2124-1 от 27 декабря 1991 г., в редакции от 27 декабря 1995 г.);
Закон РФ «Об авторском праве и смежных правах» (№5351-1 от 9 июля 1993 г., в редакции от 19 июля 1995 г.);
Федеральный закон «О связи» (№15-ФЗ от 16 февраля 1995 г.);
Федеральный закон «Об информации, информатизации и защите информации» (№24-ФЗ от 20 февраля 1995 г.);
Федеральный закон «Об участии в международном информационном обмене» (№85-ФЗ от 4 июля 1996 г.);
Федеральный закон «О рекламе» (№108-ФЗ от 18 июля 1995 г.).

США
Существующее законодательство США предусматривает наказания за совершенные преступные деяния с компьютерной информацией, телекоммуникационными сетями и компьютерными системами.

Ниже приведен перечень существующих федеральных законов в США, записанных в Кодексе Соединенных Штатов, относящихся к различным аспектам преступной информационной деятельности:

15 U.S.C. §1644 (преступления с кредитными карточками);
17 U.S.C. §506 (преступное копирование);
17 U.S.C. §1201 (защита авторских прав);
18 U.S.C. §§1028, 1029, 1030 (преступления в связи с идентификацией документов и информации, преступления в связи с получением доступа, преступления с компьютерами);
18 U.S.C. §1341 (почтовые и банковские преступления);
18 U.S.C. §2701 (незаконный доступ к коммуникациям);
18 U.S.C. §1831 (защита секретов торговли);
18 U.S.C. §§2318-2320 (передача копий компьютерных программ или компьютерной документации, копии картин или других аудио-, видеоработ).

Так, закон 18 U.S.C. §2701 о незаконном доступе к коммуникациям предусматривает наказание:
а) за намеренный доступ без получения авторизации — штраф или заключение в тюрьму на срок не более чем на год;
б) за намеренный доступ с получением расширенных полномочий — заключение в тюрьму на срок не более чем на два года.

Преступления, связанные с компьютерами, подпадают под действие статьи закона 18 U.S.C. §1030 «Намеренный доступ к компьютеру без авторизации и получение:
1) информации, содержащей финансовые записи финансовых институтов или файлов о номерах кредитных карточек, наказывается заключением в тюрьму на срок не более 10 лет;
2) информации из любого министерства или агентства США наказывается заключением в тюрьму на срок не более 20 лет;
3) информации из защищенных компьютеров наказывается заключением в тюрьму на срок не более 5 лет».

В 1998 г. в США вступил в силу федеральный закон, известный как Communcations Decency Act, в котором предусматривается ответственность администраторов-провайдеров и администраторов серверов глобальных открытых сетей за содержание размещенной у них информации.

Однако в апреле 2000 г. американский суд постановил, что компьютерные программы подпадают под закон о защите свободы слова. Тем самым теперь даже те, кто распространяет хакерские программы, могут найти поддержку в законе о защите свободы слова.

Канада

В Канаде принят закон о защите персональных данных и электронных документов под названием The Personal Information and Electronic Documents Act. Закон обеспечивает защиту персональной информации, которая собирается и используется в частном секторе. Канада уже имеет федеральное и провинциальное законодательство, защищающее персональные данные, которые используются правительством. Провинция Квебек утвердила законодательство, которое относится к частному сектору.

К персональной информации закон относит такие данные, как раса, национальность, возраст, брачный статус, религия, образование, медицинские данные, данные о трудоустройстве и финансах, адрес, телефонный номер, номер карточки социального страхования, отпечатки пальцев, группа крови, взгляды и персональное мнение. Этим законом предусматривается наказание за изменение или разрушение таких данных штрафом максимум в 100 тыс. долл.

Уголовная ответственность за информационные правонарушения предусмотрена и в Уголовном кодексе Канады.

Статья 342.1 (Несанкционированное использование компьютера) предусматривает наказание за незаконное использование компьютеров для получения, например, номеров кредитных карточек, — заключение в тюрьму сроком до 10 лет.

Статья 430.1.1 (Нарушение целостности данных, которое может привести к отказу в обслуживании законных пользователей), а также статья 326.1 (Кража телекоммуникационных услуг) предусматривают штраф или заключение в тюрьму сроком до двух лет.

Китай

Постановлением правительства КНР, названным «Временное регулирование Китайской Народной Республикой глобальной связи через компьютерную информационную сеть», устанавливается контроль всего выходящего из страны трафика. Вводятся определенные ограничения на работу компаний, которые обязаны пропускать свой трафик через бюро почты и телекоммуникаций. Создание любой новой сети, имеющей доступ в международные сети, требует получения разрешения правительства. Правительство оставляет за собой право цензуры на информацию, поступающую в страну. Китай блокирует передачу политической информации из интернета пользователям своей страны.

Китайское правительство запретило онлайновую торговлю импортной музыкой и видеофильмами. Интернет-компаниям, инвестируемым из-за рубежа, вообще запрещено продавать какую-либо аудиовизуальную продукцию. Такая торговля разрешена только тем, кто получит специальную лицензию министерства культуры Китая.

Данные меры, по словам представителей китайского правительства, направлены на «предотвращение пиратства» и «развитие здорового рынка»; за нарушение этих правил граждане Китая подлежат различным наказаниям.

Кроме того, в КНР действует запрет на импорт программного обеспечения, использующего «неизвестные Китаю» механизмы шифрования.

Франция

Национальная ассамблея Франции приняла законопроект об обязательной регистрации владельцев всех веб-сайтов страны и об уголовной ответственности провайдеров за предоставление хостинга неидентифицированным пользователям. Соответственно, все авторы сайтов, размещаемых на французских серверах, должны представлять свои личные данные провайдерам до того, как сайт появится в сети. За предоставление неполных или неверных сведений о себе пользователи подлежат наказанию тюремным заключением на срок до шести месяцев.

При этом ответственность ложится и на провайдеров: тем, кто предоставит место на сервере неидентифицированным пользователям, также грозит полгода тюрьмы.

Швейцария

Рабочая группа по изучению юридических вопросов, связанных с интернетом, министерства юстиции Швейцарии выработала следующие рекомендации для провайдеров.

1. Если провайдер располагает конкретной информацией, дающей основания подозревать, что конкретное содержание сети может быть незаконным, он должен немедленно провести расследование и блокировать доступ к этому содержанию в случае необходимости. В случае если имеются сведения, что информация незаконна, то провайдер должен принять технические меры по блокированию доступа к этому содержанию.

2. Провайдерам рекомендуется создать центр для сбора и анализа информации от провайдеров, их клиентов и прочих лиц о незаконном содержании.

3. Провайдерам рекомендуется заключать соглашения на обслуживание только со взрослыми и самостоятельными лицами. Клиенты должны иметь доступ к сети только через идентификацию и пароль.

4. В контракте провайдеры должны зарезервировать за собой право временно «замораживать» подозрительные источники информации и в одностороннем порядке разрывать контракт, если клиент распространяет незаконное содержание или если это содержание может быть получено с его компьютеров.

5. Контракт на обслуживание должен в явном виде приглашать потребителей сообщать о незаконном содержании сети и любых других незаконных приложений, о которых им стало известно.

6. Провайдеры должны знать, что наказание за показ сцен насилия по статьям Уголовного кодекса Швейцарии не ограничивается кино- или фотоизображениями, но распространяется и на другие формы представления, особенно в компьютерных играх. Это же положение относится к порнографии и наказывается штрафами или заключением в тюрьму на срок не более двух лет.

7. Провайдеры должны информировать потребителей о потенциальных проблемах, связанных с защитой данных, используемых в интернете. Необходимо также особое внимание уделять мерам по сохранению конфиденциальности и точности персональных данных, ограничению доступа к ним.

8. Провайдер должен обрабатывать только персональные данные потребителя, необходимые для обеспечения его услугами. Следует принять все необходимые технические и организационные меры, чтобы эта информация была доступна только персоналу для выполнения им необходимых работ. Недопустимо использование персональных данных в других целях. Данные могут предоставляться третьим лицам только с согласия потребителей.

9. Провайдерам не следует делать доступными телефоны, адреса и имена клиентов по интернету без их согласия за исключением случаев, когда на это есть законные основания или имеется значительный общественный интерес.

10. Необходимо иметь в виду рекомендацию 1, в случае если провайдер знает, что конкретное содержание какой-либо сети нарушает авторские права.

11. Провайдеру следует особое внимание в договоре об услугах уделять обязанностям клиента по соблюдению авторских прав и сохранять за собой возможность временно прекращать доступ к источнику нарушения авторских прав и в одностороннем порядке прекращать контракт в случае таких нарушений.

Швеция

В мае 1998 г. Парламентом Швеции принят закон «Electronic Bulletin Board», который предполагает применять государственное правовое регулирование к большинству служб, предоставляющих информацию через интернет, такие как: www-службы, серверы новостей и др. Этот закон является попыткой повторить похожий закон США Communications Decency Act, в котором предусматривается ответственность администраторов-провайдеров и администраторов серверов за содержание размещенной у них информации.

Законом вводится определение электронных сообщений (текст, изображение, звук и другие информационные форматы) и определяется перечень пользователей, к которым этот закон не применим (государственные агентства и законные группы компаний, службы, подпадающие под действие закона о свободе прессы — Freedom of the Press Act — и под действие конституции Швеции). Законом также определяются обязанности собственника электронной доски объявлений и администратора сетевого сервера. Определены также незаконные с точки зрения размещения в сети сообщения (об уголовных деяниях — раздел 16, параграф 5; о расовой агитации — раздел 16 параграф 8; о детской порнографии — раздел 16 параграф 10; призыв к насилию — раздел 16 параграф 10 и др.).

Закон предусматривает уголовное наказание за ряд действий пользователей: лицо, которое намеренно или по небрежности игнорировало обязанности собственника электронной доски объявлений должна будет уплатить штраф, то же в отношении размещения незаконных сообщений наказывается в первый раз уплатой штрафа или заключается в тюрьму на срок до шести месяцев, если преступление будет серьезней, то заключение в тюрьму на срок до двух лет. Кроме того, предусматривается конфискация (полная или частичная) компьютеров и другого оборудования, если они были использованы в преступлении.

ПРИЛОЖЕНИЕ 4. ДОКУМЕНТЫ ГЕНЕРАЛЬНОЙ АССАМБЛЕИ ООН ПО ВОПРОСУ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Письмо Постоянного представителя Российской Федерации при Организации Объединенных Наций от 23 сентября 1998 г. на имя Генерального секретаря

Настоящим имею честь направить Вам письмо Министра иностранных дел Российской Федерации И.С. Иванова от 23 сентября 1998 года на Ваше имя (см. приложение).

Буду признателен за распространение текста настоящего письма и приложения к нему в качестве документа Генеральной Ассамблеи по пункту 63 повестки дня.

С. Лавров

Приложение

Письмо Министра иностранных дел Российской Федерации от 23 сентября 1998 г. на имя Генерального секретаря

На протяжении ряда лет Генеральная Ассамблея рассматривает на своих сессиях вопрос «роль науки и техники в контексте международной безопасности, разоружения и других связанных с этим областей». Мы считаем, что этот вопрос по-прежнему актуален и, более того, приобретает в последнее время новое звучание в связи с наблюдаемым во всем мире качественно новым этапом научно-технической революции — стремительным развитием и внедрением новых информационных технологий и средств телекоммуникаций. Информационная революция, проникая практически во все сферы жизнедеятельности общества, открывает самые широкие перспективы для ускоренного и гармоничного развития всей мировой цивилизации, расширяет поле взаимовыгодного сотрудничества государств, способствует резкому увеличению созидательного потенциала человечества. Сегодня можно говорить о формировании поистине глобального и информационного пространства международного сообщества, в котором информация приобретает свойства ценнейшего элемента как национального, так и общечеловеческого достояния, его стратегического ресурса.

Вместе с тем необходимо принимать во внимание, возможно, пока и потенциальную, но от этого не менее серьезную опасность использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности и безопасности, соблюдением принципов неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека. На наш взгляд, такая опасность уже сейчас требует принятия превентивных мер. Нельзя допустить возникновения принципиально новой области конфронтации на международной арене, способной спровоцировать новый виток гонки вооружений на основе достижений научно-технической революции и, в итоге, отвлечь огромные ресурсы, так необходимые для целей мирного созидания и развития.

Речь идет о создании информационного оружия и опасности возникновения информационных войн, которые мы понимаем как действия одной страны, направленные на нанесение ущерба информационным ресурсам и системам другой при одновременной защите своей собственной инфраструктуры.

Беспрецедентный уровень информатизации общества и одновременно уязвимость его информационной инфраструктуры обусловливают риск появления такого информационного оружия, разрушительный «эффект» от применения которого может оказаться сравнимым с оружием массового поражения.

В этих условиях возникает и реальная угроза воздействия на информационные ресурсы в террористических или криминальных целях, последствия которого также могут иметь катастрофический характер. Все эти опасения подводят нас к выводу о том, что проблема международной информационной безопасности созрела для того, чтобы стать темой предметного и целенаправленного обсуждения в рамках Организации Объединенных Наций.

Прошу Вас рассматривать настоящее письмо как объяснительную записку, предусмотренную правилами процедуры Генеральной Ассамблеи, и распространить его вместе с прилагаемым проектом резолюции (см. добавление) в качестве документа Генеральной Ассамблеи по пункту 63 повестки дня.

И. Иванов

Добавление

Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности

Российская Федерация: проект резолюции

Генеральная Ассамблея,

ссылаясь на свои резолюции по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях;

признавая с удовлетворением значительный прогресс в разработке и внедрении новейших информационных технологий и средств телекоммуникаций;

подтверждая, что видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения поля взаимодействия государств, увеличения созидательного потенциала человечества и формирования глобального информационного пространства международного сообщества;

напоминая в этой связи о подходах и принципах создания такого сообщества, которые были намечены международной конференцией «Информационное сообщество и развитие» в Мидранде, Южная Африка, в 1996 г., отмечая, что распространение и использование информационных технологий и средств затрагивает интересы всего международного сообщества и их оптимальный учет возможен лишь в контексте широкого международного взаимодействия;

выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной безопасности и стабильности, соблюдением принципов отказа от угрозы применения силы, невмешательства во внутренние дела, уважения прав и свобод человека;

считая также необходимым предотвратить появление информационных технологий и средств, применение которых в военных целях может оказаться сравнимым с применением оружия массового поражения;

будучи озабочена возможностью использования новых информационных технологий для совершенствования существующих и создания новых систем такого оружия;

выражая обеспокоенность тем, что масштабность и одновременно уязвимость глобальной информационной структуры обусловливает реальные угрозы воздействия на нее в террористических и криминальных целях, результаты которого также могут иметь катастрофический характер;

1) *предлагает* государствам-членам Организации Объединенных Наций активизировать рассмотрение на двустороннем и многостороннем уровнях существующих потенциальных угроз в сфере информационной безопасности;

2) *призывает* Генерального секретаря и органы Организации Объединенных Наций содействовать этому процессу;

3) *приглашает* все государства-члены информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:
a) общий взгляд на проблемы использования информационных технологий в военных целях;
b) определение понятий «информационное оружие», «информационная война», другое враждебное или несанкционированное воздействие на информационно-телекоммуникационные системы и информационные ресурсы;
c) целесообразность разработки международно-правовых режимов запрещения разработки, производства и применения особо опасных видов информационного оружия, а также борьбы с информационным терроризмом и криминалом, включая создание международной системы (центра) мониторинга угроз, связанных с безопасностью глобальных информационно-телекоммуникационных систем;

4) *просит* Генерального секретаря обобщить взгляды и оценки по проблемам информационной безопасности и представить доклад Генеральной Ассамблее на ее пятьдесят четвертой сессии;

5) *постановляет* включить в предварительную повестку дня своей пятьдесят четвертой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности».

Источник: Док. Генеральной Ассамблеи ООН A/C. 1/53/3, 30 сентября 1998.

Резолюция Генеральной Ассамблеи ООН 53/70

Генеральная Ассамблея,

ссылаясь на свои резолюции по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях;

отмечая значительный прогресс в разработке и внедрении новейших информационных технологий и средств телекоммуникации;

подтверждая, что она видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения возможностей взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе;

напоминая в этой связи о принципах, которые были намечены на конференции «Информационное сообщество и развитие», состоявшейся в Мидранде, Южная Африка, 13-15 мая 1996 г.;

принимая к сведению итоги Совещания на уровне министров по проблеме терроризма, которое состоялось в Париже 30 июля 1996 г., а также принятые на нем рекомендации[1];

отмечая, что распространение и использование информационных технологий и средств затрагивает интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности;

выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на безопасность государств;

считая необходимым предотвратить неправомерное использование или использование информационных ресурсов или технологий в преступных или террористических целях;

[1] См.: A/51/261, приложение.

1) *призывает* государства-члены содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности;

2) *просит* все государства-члены информировать Генерального секретаря о своей точке зрения и оценках по следующим вопросам:
a) общая оценка проблем информационной безопасности;
b) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов;
c) целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и криминалом;

3) *просит* Генерального секретаря представить доклад Генеральной Ассамблее на ее пятьдесят четвертой сессии;

4) *постановляет* включить в предварительную повестку дня своей пятьдесят четвертой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности».

Источник: Док. Генеральной Ассамблеи ООН A/RES/53/70, 4 декабря 1998.

Резолюция Генеральной Ассамблеи ООН 54/49

Генеральная Ассамблея,

ссылаясь на свою резолюцию 53/70 от 4 декабря 1998 г.;

ссылаясь также на свои резолюции по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях;

отмечая значительный прогресс в разработке и внедрении новейших информационных технологий и средств телекоммуникации;

подтверждая, что она видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения возможностей взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе;

напоминая в этой связи о подходах и принципах, которые были намечены на конференции «Информационное сообщество и развитие», состоявшейся в Мидранде, Южная Африка, 13-15 мая 1996 г.;

принимая к сведению итоги Совещания на уровне министров по проблеме терроризма, которое состоялось в Париже 30 июля 1996 г., а также принятые на нем рекомендации[2];

отмечая, что распространение и использование информационных технологий и средств затрагивает интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности;

выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на безопасность государств применительно как к гражданской, так и к военной сфере;

считая необходимым предотвратить неправомерное использование или использование информационных ресурсов или технологий в преступных или террористических целях;

отмечая вклад государств-членов, представивших Генеральному секретарю свои оценки по вопросам информационной безопасности в соответствии с пунктами 1-3 ее резолюции 53/70;

принимая к сведению доклад Генерального секретаря, содержащий эти оценки[3];

оценивая своевременную инициативу Секретариата и Института Организации Объединенных Наций по исследованию проблем разоружения по проведению международной встречи экспертов в Женеве

[2] См.: A/51/261, приложение.
[3] См.: A/54/213.

в августе 1999 г. по теме «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»;

считая, что оценки государств-членов, содержащиеся в докладе Генерального секретаря, а также международная встреча экспертов способствовали лучшему пониманию существа проблем международной информационной безопасности, связанных с ними понятий и возможных мер ограничения возникающих в этой сфере угроз;

1) *призывает* государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности;

2) *просит* все государства-члены продолжать информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:
a) общая оценка проблем информационной безопасности;
b) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов;
c) целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и криминалом;

3) *просит* Генерального секретаря представить доклад Генеральной Ассамблее на ее пятьдесят пятой сессии;

4) *постановляет* включить в предварительную повестку дня своей пятьдесят пятой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности».

Источник: Док. Генеральной Ассамблеи ООН A/RES/54/49, 1 декабря 1999.

Резолюция Генеральной Ассамблеи ООН 55/28

Генеральная Ассамблея,

ссылаясь на свои резолюции 53/70 от 4 декабря 1998 г. и 54/49 от 1 декабря 1999 г.;

напоминая о своих резолюциях по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях;

отмечая значительный прогресс в разработке и внедрении новейших информационных технологий и средств телекоммуникации;

подтверждая, что она видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения возможностей взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе;

напоминая в этой связи о подходах и принципах, которые были намечены на конференции «Информационное сообщество и развитие», состоявшейся в Мидранде, Южная Африка, 13-15 мая 1996 г.;

учитывая итоги Совещания на уровне министров по проблеме терроризма, которое состоялось в Париже 30 июля 1996 г., а также принятые на нем рекомендации[4];

отмечая, что распространение и использование информационных технологий и средств затрагивает интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности;

выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на безопасность государств применительно как к гражданской, так и к военной сферам;

отмечая вклад государств-членов, представивших Генеральному секретарю свои оценки по вопросам информационной безопасности в соответствии с пунктами 1-3 резолюций 53/70 и 54/49;

принимая к сведению доклады Генерального секретаря, содержащие эти оценки[5];

---

[4] См.: A/51/261, приложение.
[5] См.: A/54/213, A/55/140, Corr.1 и Add.1.

отмечая с удовлетворением инициативу Секретариата и Института Организации Объединенных Наций по исследованию проблем разоружения по проведению международной встречи экспертов в Женеве в августе 1999 г. по теме «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», а также ее результаты;

считая, что оценки государств-членов, содержащиеся в докладах Генерального секретаря, а также международная встреча экспертов способствовали лучшему пониманию существа проблем международной информационной безопасности и связанных с ними понятий;

1) *призывает* государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также рассмотрению возможных мер по ограничению угроз, возникающих в этой сфере;

2) *полагает*, что целям таких мер соответствовало бы изучение соответствующих международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем;

3) *просит* все государства-члены продолжать информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:
a) общая оценка проблем информационной безопасности;
b) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или противоправное использование информационных и телекоммуникационных систем и информационных ресурсов;
c) содержание концепций, упомянутых в пункте 2 настоящей резолюции;

4) *просит* Генерального секретаря на основе полученных ответов государств-членов представить доклад Генеральной Ассамблее на ее пятьдесят шестой сессии;

5) *постановляет* включить в предварительную повестку дня своей пятьдесят шестой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

Источник: Док. Генеральной Ассамблеи ООН A/RES/55/28, 20 ноября 2000.

Резолюция Генеральной Ассамблеей 55/63

Генеральная Ассамблея,

ссылаясь на Декларацию тысячелетия Организации Объединенных Наций[6], в которой государства-члены провозглашают решимость обеспечить, чтобы благами новых технологий, особенно информационно-коммуникационных технологий, в соответствии с рекомендациями, содержащимися в декларации министров, принятой на этапе заседаний высокого уровня основной сессии Экономического и Социального Совета 2000 г.[7], могли пользоваться все;

ссылаясь также на свою резолюцию 45/121 от 14 декабря 1990 г., в которой она одобрила рекомендации восьмого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями[8], и отмечая, в частности, его резолюцию о преступлениях, связанных с применением компьютеров[9], в которой восьмой Конгресс призвал государства активизировать усилия, направленные на более эффективную борьбу с преступлениями, связанными с применением компьютеров;

подчеркивая тот вклад, который Организация Объединенных Наций, в особенности Комиссия по предупреждению преступности и уголовному правосудию, может внести в дело поощрения более действенной и эффективной работы правоохранительных органов и системы отправления правосудия и самых высоких стандартов справедливости и человеческого достоинства;

признавая, что свободное движение информации может способствовать экономическому и социальному развитию, образованию и демократическому управлению;

отмечая значительный прогресс в разработке и внедрении информационных технологий и телекоммуникационных средств;

---

[6] См.: резолюцию 55/2.

[7] См.: A/55/3, глава III. Окончательный текст см.: Официальные отчеты Генеральной Ассамблеи, пятьдесят пятый год. Дополнение №3.

[8] Восьмой Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Гавана. 27 августа — 7 сентября 1990 г. Доклад, подготовленный Секретариатом. Глава 1. Издание Организации Объединенных Наций, №R.91.1V.2.

[9] Там же, раздел C, резолюция 9.

выражая обеспокоенность в связи с тем, что технический прогресс создал новые возможности для преступной деятельности, и в частности для преступного использования информационных технологий;

отмечая, что повсеместное распространение информационных технологий, масштабы использования которых в разных государствах могут быть различными, привело к значительному росту глобального сотрудничества и координации, в результате чего преступное использование информационных технологий может иметь серьезные последствия для всех государств;

признавая, что несоответствия в уровне доступа различных государств к информационным технологиям и их использования могут снизить эффективность международного сотрудничества в борьбе с преступным использованием информационных технологий, и отмечая необходимость содействия передаче информационных технологий, в частности развивающимся странам;

отмечая необходимость предупреждения преступного использования информационных технологий;

признавая необходимость сотрудничества между государствами и частным сектором в борьбе с преступным использованием информационных технологий;

подчеркивая необходимость усиления координации и укрепления сотрудничества между государствами в борьбе с преступным использованием информационных технологий и отмечая в этом контексте ту роль, которую могут сыграть Организация Объединенных Наций и региональные организации;

приветствуя работу десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями[10];

отмечая работу Комитета экспертов Совета Европы по преступлениям в информационном пространстве над проектом конвенции об информационной преступности, принципы, согласованные министрами юстиции и внутренних дел «Группы восьми» в Вашингтоне, округ

[10]См.: Доклад десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, состоявшегося в Вене 10-17 апреля 2000 г. Док. A/CONF.187/15.

Колумбия, 10 декабря 1997 г. и поддержанные 17 мая 1998 г. главами государств «Группы восьми» в Бирмингеме, Соединенное Королевство Великобритании и Северной Ирландии, работу Конференции «Группы восьми» по проведению диалога между правительствами и промышленностью о безопасности и доверии в информационном пространстве, состоявшейся в Париже 15-17 мая 2000 г., и принятые 2 марта 2000 г. рекомендации третьего Совещания министров юстиции, министров и генеральных прокуроров государств Американского континента, созванного в рамках Организации американских государств в Сан-Хосе, Коста-Рика, 1-3 марта 2000 г.[11];

1) *с удовлетворением отмечает* усилия этих организаций по предупреждению преступного использования информационных технологий и отмечает также важность, в частности, следующих мер по борьбе с таким использованием информационных технологий:
a) государства должны обеспечить, чтобы их законодательство и практика не оставляли возможности тем, кто злоупотребляет информационными технологиями, укрываться где бы то ни было;
b) сотрудничество правоохранительных органов в расследовании случаев трансграничного преступного использования информационных технологий и судебном преследовании в этой связи должно координироваться всеми соответствующими государствами;
c) государства должны обмениваться информацией о проблемах, с которыми они сталкиваются в борьбе с преступным использованием информационных технологий;
d) сотрудники правоохранительных органов должны быть обучены и оснащены для борьбы с преступным использованием информационных технологий;
e) правовые системы должны защищать конфиденциальность, целостность и доступность данных и компьютерных систем от несанкционированного вмешательства и предусматривать наказания за злоупотребления, совершаемые в преступных целях;
f) правовые системы должны обеспечивать сохранность электронных данных, имеющих отношение к расследованию конкретных преступлений, и быстрый доступ к ним;
g) режимы взаимной помощи должны обеспечивать своевременное расследование случаев преступного использования информационных технологий и своевременный сбор доказательств и обмен ими в подобных случаях;

[11]См.: REMJA-lll/doc.l4/00 rev.2, глава IV

h) общественность должна быть осведомлена о необходимости предупреждения преступного использования информационных технологий и борьбы с ним;
i) насколько это практически осуществимо, информационные технологии должны разрабатываться таким образом, чтобы содействовать предупреждению и обнаружению случаев преступного использования, отслеживанию преступников и сбору доказательств;
j) борьба с преступным использованием информационных технологий требует выработки решений, учитывающих как необходимость защиты личных свобод и частной жизни, так и сохранения у правительств возможности бороться с подобным явлением;

2) *призывает* государства учитывать эти меры в предпринимаемых ими усилиях по борьбе с преступным использованием информационных технологий;

3) *постановляет* сохранить в повестке дня своей пятьдесят шестой сессии вопрос о преступном использовании информационных технологий в рамках пункта, озаглавленного «Предупреждение преступности и уголовное правосудие».

Источник: Док. Генеральной Ассамблеи ООН A/RES/55/63, 4 декабря 2000.

Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности
Доклад Генерального секретаря

Содержание

Введение

1. В пунктах 2 и 3 своей резолюции 53/70 от 4 декабря 1998 г., озаглавленной «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», Генеральная Ассамблея просила все государства-члены информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам: a) общая оценка проблем информационной безопасности; b) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов; и c) целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и криминалом; и просила Генерального секретаря представить ей доклад на ее пятьдесят четвертой сессии.

2. 19 марта 1999 г. Генеральный секретарь направил в адрес государств-членов вербальную ноту, в которой предложил им представить свою точку зрения во исполнение просьбы Ассамблеи. Ответы, полученные от правительств, воспроизводятся ниже.

Ответы, полученные от правительств

Австралия

Подлинный текст на английском языке
2 июня 1999 г.

1. Австралия председательствовала в Группе экспертов Организации экономического сотрудничества и развития (ОЭСР), которая подготовила Руководящие принципы ОЭСР по обеспечению безопасности информационных систем. Австралия председательствует также в Рабочей группе ОЭСР по вопросам информационной безопасности и тайны, которая среди прочих своих обязанностей следит за необходимостью обеспечения информационной безопасности. Австралия участвует в разработке норм безопасности информационной технологии в рамках Международной организации по стандартизации (МОС). Внутри страны введены детальные процедуры обеспечения безопасности правительственной информации, и Госстандарт Австралии совместно с Госстандартом Новой Зеландии разработали на базе английского стандарта совместный стандарт управления информационной безопасностью. Правительство и промышленность Австралии занимаются в настоящее время совместной разработкой мер по охране национальной информационной

инфраструктуры. В Австралии принято законодательство, обеспечивающее защиту телекоммуникационных систем от перехвата, вмешательства и других форм неправомерного использования.

2. Задача информационной безопасности, как она изложена в Руководящих принципах ОЭСР по обеспечению безопасности информационных систем и применяется на практике Австралией, заключается в следующем: «... защита интересов сторон, полагающихся на информационные системы, от причинения вреда в результате нарушения доступности, конфиденциальности и неприкосновенности».

3. По мере сближения технологий данная задача может быть распространена на телекоммуникационные системы, являющиеся частным случаем информационной системы. Любое вмешательство или неправомерное использование информационных систем отразится либо на доступности, либо на конфиденциальности, либо на неприкосновенности. В условиях быстрого технического прогресса существует опасность выработки определений, слишком тесно привязанных к конкретным технологиям.

4. Австралия не разделяет мнения о том, что Департамент по вопросам разоружения Секретариата Организации Объединенных Наций является подходящим органом для разработки международных принципов обеспечения безопасности глобальных информационных и телекоммуникационных систем. Телекоммуникации и информационная инфраструктура оказывают влияние на вопросы торговли, экономического развития и общественного благосостояния, а также охраны правопорядка и национальной безопасности. Принципы и руководящие указания по этим вопросам уже разработаны на других форумах, таких как ОЭСР, МОС и Международный союз электросвязи (МСЭ), с применением более широких подходов, чем подходы, предложенные в резолюции 53/70 Генеральной Ассамблеи. Кроме того, решением вопросов компьютерных преступлений занимаются такие международные органы, как Азиатский и дальневосточный институт Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями (ЮНАФЕИ) и Центр по международному предупреждению преступности. Австралия не видит смысла в том, чтобы другие органы Организации Объединенных Наций дублировали работу, которая проводится в настоящее время в мире в связи с вопросами безопасности или неправомерного использования компьютерной техники. Австралия поддержала бы предложение о развитии информационного ресурса работы, осуществляемой в рамках других форумов.

Беларусь

Подлинный текст на английском языке
25 мая 1999 г.

1. Республика Беларусь полностью поддерживает резолюцию 53/70 Генеральной Ассамблеи от 4 декабря 1998 г., озаглавленную «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». Активное применение новых информационных технологий и средств телекоммуникации открывает широчайшие возможности для ускоренного развития мировой цивилизации. В то же время, как указано в резолюции 53/70 Ассамблеи, «эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на безопасность государств».

2. Принятие резолюции 53/70 Ассамблеи является своевременным и актуальным, поскольку позволяет привлечь внимание международного сообщества к потенциальному использованию информационных технологий ведения войны и необходимости недопущения новых информационных технологий и средств, военное применение которых можно сравнить с оружием массового поражения. Кроме того, после принятия резолюции 53/70 Генеральной Ассамблеи появилась возможность конкретного рассмотрения проблемы международной информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов. Наконец, целесообразно разработать и согласовать концепцию международной информационной безопасности и международно-правовые принципы, направленные на укрепление безопасности глобальных информационных и телекоммуникационных систем и предупреждение информационного терроризма и преступности.

Бруней-Даруссалам

Подлинный текст на английском языке
7 июня 1999 г.

В связи с резолюцией 53/70 Генеральной Ассамблеи от 4 декабря 1998 г., озаглавленной «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». Постоянное представительство Брунея-Даруссалама имеет честь представить следующую точку зрения министерства обороны Брунея-Даруссалама:

«Министерство обороны как министерство, ведающее вопросами национальной обороны, признает важность информационной

безопасности в современную эпоху информационной технологии. Министерство считает важным любую форму информации, которая может быть использована и может создавать угрозу национальной безопасности при ее передаче. Однако благодаря имеющимся у него связям с информационной технологией и благодаря наличию в стране других министерств, занимающихся этим вопросом, министерство обороны будет сотрудничать с соответствующими учреждениями в осуществление положений указанной резолюции. В интересах обеспечения и создания гарантий безопасности международных коммуникаций ответственность в данном вопросе не следует считать выходящей за рамки компетенции Международного Суда».

Куба

Подлинный текст на испанском языке
28 июня 1999 г.

Общая оценка проблем информационной безопасности

1. Широкое использование информационных технологий практически во всех сферах деятельности человека, т.е. процесс «компьютеризации общества», который многие называют «информационным веком» как отражение растущей зависимости от информационных систем в мире, создает новые проблемы безопасности, требующие самого серьезного рассмотрения не только отдельными государствами, но и всем международным сообществом.

2. По этой причине Организация Объединенных Наций является подходящим форумом для обсуждения соответствующих путей и средств преодоления потенциальных угроз для международной безопасности, которые могут возникать в связи с использованием новых информационных и телекоммуникационных технологий в немирных целях.

3. Кроме того, должны приниматься меры для обеспечения доступности этих технологий в целях развития всех государств, особенно слаборазвитых государств, которые не имеют достаточных ресурсов для самостоятельной разработки таких технологий.

4. В то же время процесс глобализации в сфере информатизации и телекоммуникации уже стал реальностью, и расстояния больше не являются препятствием для обмена информацией; в то же время безопасность систем, способствующих обмену информацией, вызывает растущее беспокойство. Следует подчеркнуть, что следствием глобализации является определенный уровень стандартизации, облегчающий вмешательство в эти системы.

5. Не следует забывать о том, что речь идет о технологиях, создаваемых в развитых странах, среди которых Соединенные Штаты Америки, крупнейшая в мире гегемонистская держава, особенно в области информатизации и телекоммуникации, занимает доминирующее положение, позволяющее ей навязывать технологические стандарты, облегчающие использование информационных и телекоммуникационных систем как средство агрессии.

6. Так что у слаборазвитых стран нет другой альтернативы, кроме как принять эти технологии, чтобы выжить в новых условиях. В большинстве случаев эти страны не вполне осознают таящуюся в этом опасность и во многих случаях недостаточно широко используют меры, службы или механизмы обеспечения безопасности. Результатом является уязвимость информационных систем, которая в условиях широкого использования информационных и телекоммуникационных технологий во всех сферах общественного развития может вести к возникновению ситуаций, угрожающих международной безопасности.

7. Куба весьма признательна за предоставленную возможность рассмотреть данный пункт на Генеральной Ассамблее благодаря инициативе, приведшей к принятию консенсусом резолюции 53/70 Ассамблеи. Куба сознает важность данного пункта и будет активно участвовать в проведении оценок, предусмотренных в этой резолюции.

Определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов

8. В современном мире наблюдается беспрецедентный рост использования информационных и телекоммуникационных технологий, который, к сожалению, сделал возможным их использование во враждебных целях для проведения одними государствами агрессивной политики в отношении других государств.

9. В этой связи следует указать, что развитие и популярность глобальных сетей, особенно интернета, имеет серьезные последствия. Несмотря на их растущее использование, информационные и телекоммуникационные системы по-прежнему функционируют на чисто кооперативной основе. Это важный момент, поскольку добровольный характер интернета является одновременно источником его сильных и самых слабых качеств.

10. Общий свод правил, обеспечивающих эффективную и повышенную оперативную безопасность глобальных сетей, носит добровольный характер в силу того факта, что страны не приняли единообразного законодательства в отношении функционирования информационных сетей.

11. Однако, поскольку участие в таких глобальных сетях является факультативным, можно с полным основанием утверждать, что любые правила поведения, регулирующие функционирование таких сетей, должны быть составной частью соглашения об участии и что нарушение таких правил, независимо от имеющейся правовой инфраструктуры, может повлечь за собой применение санкций.

12. Безопасность информации включает защиту ее конфиденциальности (информация должна быть доступна только тем, кто имеет право на ее использование), защиту информации от несанкционированного изменения (неприкосновенность) и защиту систем от отказа в обслуживании (доступность) и несанкционированного доступа.

13. В этой связи следует рассмотреть ряд основных критериев:
a) пользователи несут ответственность за свое собственное поведение; иными словами, несанкционированный доступ к компьютеру или несанкционированное использование сети является явным нарушением правил поведения, независимо от того, насколько слабо могут быть защищены информационные системы;
b) организации, пользующиеся этими технологиями, несут ответственность за их надлежащее использование своими сотрудниками и, следовательно, должны разрабатывать с этой целью политику обеспечения безопасности, а также меры и процедуры, обеспечивающие контроль за ее соблюдением. Аналогичным образом, в каждой стране следует создать надлежащие механизмы, обеспечивающие соблюдение этих требований базирующимися на их территории организациями;
c) поставщики компьютерных услуг и сетей несут ответственность за обеспечение безопасности своих систем. Они несут также ответственность за информирование пользователей о своей политике обеспечения безопасности и о любых изменениях в такой политике;
d) продавцы и поставщики систем несут ответственность за обеспечение их надежного функционирования, предусматривающего надлежащие меры обеспечения безопасности. Продавец или поставщик должны оценивать каждую систему до ее выпуска на рынок с точки зрения мер обеспечения безопасности. К каждому товару должно прилагаться описание предусмотренных в нем мер безопасности. Продавцы и поставщики

систем обязаны бесплатно устранять дефекты в соответствующих компонентах продаваемых или распространяемых ими систем;
e) пользователи, поставщики услуг и продавцы программного обеспечения и аппаратных средств должны сотрудничать друг с другом в деле обеспечения безопасности. Следует надеяться, что каждый сайт будет уведомлять другие сайты об установленных случаях несанкционированного доступа и что они будут оказывать друг другу помощь в принятии мер по борьбе с нарушениями безопасности. Такая помощь может включать отслеживание связей, выявление нарушений и оказание правовой помощи.

14. Лица, вторгающиеся в информационные сети, преследуют следующие основные цели:
a) получение, изменение или уничтожение информации. Это, несомненно, главная цель большинства нарушителей;
b) проникновение в чужие компьютеры и их использование под видом санкционированных пользователей;
c) создание плацдарма для дальнейших нарушений. Вторжение в системы может преследовать единственную цель их использования в качестве основы для новых вторжений;
d) отказ в обслуживании, т.е. отказ в предоставлении информации лицам, которые в ней нуждаются и имеют право на ее использование;
e) самореклама, что весьма выгодно в случае использования Web-серверов.

15. Неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов, особенно при использовании таких систем и ресурсов некоторыми государствами для проведения своей политики и вмешательства в дела других государств, является нарушением суверенитета и независимости соответствующих государств и создает очаги напряженности, которые могут представлять серьезную угрозу для международной безопасности.

16. Государства, постоянно добивающиеся достижения политических целей в своих национальных интересах, занимаются, с точки зрения установленных международных норм, неправомерным использованием, в частности, радио- и телевизионных станций с целью дестабилизации конституционного порядка других государств, которых они считают своими врагами.

17. Куба является примером государства, по отношению к которому проводится упомянутая в предыдущих пунктах политика. О серьезности этого вопроса можно судить по тому, что Куба в течение многих десятилетий является объектом агрессии со стороны американского радио

и телевидения, являющихся составной частью целенаправленной агрессивной политики, проводимой этой самой развитой в военном, экономическом и политическом отношении державой мира, которая объявила своей целью свержение правительства Кубы.

18. С этой целью, например, до апреля 1999 г. на территории Соединенных Штатов Америки работало в общей сложности 17 радиостанций, которые передавали на Кубу информацию подрывного содержания.

19. Ежедневный объем радиовещания составлял от 288,5 до 306,5 часов в диапазоне средних, коротких и ультракоротких волн; еженедельная продолжительность радиовещания составляла 2084,5 часов, а если добавить к этому еженедельный объем телевизионных трансляций, то эта цифра составит в общей сложности 2089 часов.

20. В большинстве случаев передаваемая информация подстрекала кубинских граждан к совершению актов гражданского неповиновения и к участию в подрывных и террористических акциях.

21. Куба всегда выступала за устранение разногласий между государствами на основе равенства и уважения их национального суверенитета и независимости и неоднократно делала на этот счет публичные заявления. Эта позиция остается неизменной.

Целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и преступностью

22. Развитие новых информационных технологий, несомненно, требует параллельных усилий по обеспечению прогрессивного развития международного права в этой области, включая разработку надлежащей нормативно-правовой базы, которая была бы направлена на укрепление безопасности информационных систем.

23. Задача будет непростой, если учитывать тот факт, что до сих пор сохраняются вопросы, которые потребуют разработки общепринятых определений с целью облегчения последующей кодификации новых принципов, способствующих достижению целей в области безопасности.

24. Глобальные сети уже по одному своему определению выходят далеко за рамки юрисдикции каждой страны; во многих случаях полагаться на

географические границы становится невозможным. Кроме того, неодинаковый уровень развития государств, среди прочих факторов, серьезным образом затрудняет разработку унифицированных международных правил, которые были бы общеприменимы ко всем странам, совместно пользующимся этими технологиями.

25. Правда, работа начнется не на пустом месте, поскольку уже существуют общепринятые принципы и международно-правовые документы, которые согласовывались и принимались государствами на различных многосторонних форумах по мере происходившего в последнее время научно-технического прогресса. Эти принципы и документы оказались бы весьма полезными при составлении или разработке новых международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и преступностью.

26. Среди недавних примеров таких соглашений Куба считает необходимым упомянуть следующие:
a) резолюция 110 (II) Генеральной Ассамблеи от 3 ноября 1947 г., в которой осуждается пропаганда, имеющая целью создать или усилить угрозу миру, нарушение мира или акт агрессии;
b) Международная конвенция электросвязи, принятая в Найроби в 1982 г., а также соответствующие международно-правовые документы, принятые Организацией Объединенных Наций по вопросам образования, науки и культуры и Международным союзом электросвязи;
c) Принципы использования государствами искусственных спутников Земли для международного непосредственного телевизионного вещания, принятые Генеральной Ассамблеей, в которых предусматривается, что такая деятельность должна осуществляться в соответствии с международным правом и таким образом, чтобы она была совместимой с развитием взаимопонимания и укреплением дружественных отношений и сотрудничества между государствами и народами в интересах поддержания международного мира и безопасности;
d) Конвенция о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении, в приложении к которой содержатся положения о защите конфиденциальной информации, которые могли бы также послужить полезным справочным материалом при разработке вышеупомянутых принципов.

27. Наконец, в рамках той ведущей роли, которую следует играть Организации Объединенных Наций в возможном проведении анализа по

данному вопросу, Организация, по мнению Кубы, должна, в частности, признать тот факт, что каждая страна имеет право на защиту своих информационных и телекоммуникационных систем с помощью систем обеспечения безопасности, и рекомендовать государствам-членам принять законы, предусматривающие меры наказания за разработку и распространение компьютерных вирусов и других вредоносных программ. Кроме того, в рамках Организации Объединенных Наций могут быть заключены имеющие обязательную юридическую силу многосторонние соглашения, запрещающие агрессивные действия в отношении информационных и коммуникационных систем. Можно также рассмотреть идею заключения соглашений, гарантирующих использование разрабатываемых новых технологий в мирных целях и их доступность для всех государств.

Оман

Подлинный текст на арабском языка
22 июня 1999 г.

1. Управление телекоммуникаций Султаната не отвечает за предоставление информации подписчикам, а занимается только обеспечением сетей и технологий, облегчающих доступ к информационным системам.

2. В качестве поставщика сетей и технологий Управление проводит общую оценку проблем информационной безопасности. Безусловно, существует возможность использования предоставляемых Управлением технологий несанкционированными сторонами для получения доступа к информации, и это может иметь негативные последствия.

3. В качестве поставщика телекоммуникационных услуг Управление обычно не несет ответственности за обеспечение безопасности предоставляемой подписчикам информации, которые должны сами принимать необходимые меры предосторожности для соблюдения требований безопасности в отношении получаемой ими информации. Однако Управление может ограничить доступ к информации в общественной сфере через определенные виды служб, например интернет.

4. Что касается основных понятий, относящихся к информационной безопасности, то в действующих в Султанате правилах, и особенно правилах защиты авторского права, говорится, что информация имеет материальный и нравственный аспекты, и, следовательно, предусматривается ее правовая защита. На основе этого принципа можно

определить основные понятия, относящиеся к информационной безопасности. Наиболее важными являются следующие понятия:
a) незаконный перехват информации и данных;
b) незаконное проникновение в компьютерные системы;
c) сбор данных и информации путем шпионажа и подслушивания;
d) вторжение в частную жизнь других людей или нарушение их права на конфиденциальность;
e) предоставление любого рода данных или документов, хранящихся в электронной форме;
f) уничтожение, видоизменение и переадресование данных;
g) сбор и переадресование информации;
h) утечка информации и данных;
i) противоправное вторжение в компьютерные программы путем модификации или подделки;
j) незаконное копирование программ в нарушение прав интеллектуальной собственности;
k) кража и использование сетевых адресов;
l) изменение, дополнение или изъятие информации из передаваемого первоначального сообщения до его поступления адресату;
m) сознательное заражение вирусами и преступное изменение содержания сетевой информации;
n) фактическое (физическое) уничтожение оборудования и зданий.

5. Укрепить безопасность информационных систем можно следующими путями:
a) обучение персонала технике безопасности с разъяснением существующих опасностей и путей их предотвращения;
b) контроль за доступом; т.е. выдача различного рода разрешений лицам, имеющим санкционированный доступ к информации в конкретных категориях;
c) использование опознавательных цифровых кодов (цифровые подписи, цифровые подтверждения права доступа) для передаваемых сообщений между настоящими пользователями;
d) кодирование как аппаратных средств, так и программного обеспечения;
e) использование защитных систем для недопущения распространения информации, в которую были внесены несанкционированные изменения.
f) использование антивирусов.

6. Султанат надеется на разработку международных принципов, направленных на укрепление безопасности глобальных информационных систем, особенно с учетом введения интернета в стране, которая тем

самым оказалась подверженной рискам, связанным с обеспечением информационной безопасности.

Катар

Подлинный текст на английском языке
10 июня 1999 г.

Компетентные органы Государства Катар представили следующую информацию о своей точке зрения и оценках в отношении пунктов 2 и 3 резолюции 53/70 Генеральной Ассамблеи от 4 декабря 1998 г.:

a) общая оценка проблем информационной безопасности. Общей оценке проблем информационной безопасности могут способствовать обмен техническими знаниями и понимание опасности несанкционированного вмешательства, а также его воздействия на вопросы безопасности и финансовые вопросы;

b) определение основных понятий, относящихся к информационной безопасности. Основными понятиями, относящимися к обеспечению безопасности, являются те меры, которые необходимо соблюдать для обеспечения путей и средств обмена информацией, а также неожиданно возникающие проблемы, как наглядно показано в таблицах 1 и 2 ниже, в которых перечислены необходимые меры по обеспечению информационной безопасности на всех этапах наряду с возникающими в этой области новыми проблемами;

c) принципы, которые были бы направлены на укрепление безопасности коммуникационных систем. Укрепления информационной безопасности можно добиться путем совершенствования средств передачи информации, и наиболее важными с точки зрения обеспечения безопасности коммуникационных систем, с учетом связанных с этим больших финансовых издержек, являются следующие моменты:

i) использование нестандартных протоколов линии передачи данных, которые можно разработать специально для обмена определенными видами информации;

ii) использование системы кодирования, которая должна быть разработана для данной конкретной цели и не должна предусматривать использования программ, производимых в промышленных масштабах;

iii) внесение изменений с разными временными параметрами и кодами.

Таблица 1. Методы обеспечения безопасности компьютерных сетей. Меры по обеспечению безопасности

Угроза	Метод обеспечения безопасности	Функция
Незаконный перехват, прочтение или изменение данных	Шифрование (стандарт шифрования данных, DES, алгоритм цифровой подписи Рай веста-Шамира-Адлемана)	Кодирование данных в целях предотвращения их изменения
Лицо, имеющее право пользоваться сетью, получает несанкционированный доступ к данным	Применение программ, обеспечивающих контроль за доступом к данным	Эти программы четко определяют полномочия пользователей и контролируют осуществление этих полномочий
Пользователь преднамеренно неправильно идентифицирует себя в целях совершения мошеннических операций	Проверка права пользователя на доступ к данным	Методика, включающая применение шифровальных программ и идентификационных карт в целях установления права как отправителя, так и получателя на доступ к соответствующей информации
Не имеющий соответствующих полномочий пользователь одной из сетей получает доступ к другой сети	Применение аппаратных и программных средств сетевой защиты	Фильтруют определенные информационные потоки в целях предотвращения несанкционированного доступа к сети или серверу
Хакеры используют «дыры» в операционной системе сервера в целях получения доступа к данным и их изменения	Специальные средства операционной системы	Устраняют «дыры» в операционной системе

Таблица 2. Проблемы в области безопасности

Изменения	Проблемы
Современная сеть:	Безопасность системы находится под угрозой, поскольку:
Охватывает гораздо большее число портативных компьютеров	Портативные компьютеры легко украсть
Имеет больше беспроводных соединений	В беспроводные каналы связи можно легче проникнуть
Более обширна с географической точки зрения	Защиту удаленных узлов сложнее обеспечить
Связывает большее число разнообразных платформ	Пользователь забывает пароль или записывает несколько паролей
Все чаще бывает связанной с сетями общего пользования, такими как интернет	Хакеры «атакуют» сети общего пользования
Чаще использует компьютерные системы UNIX	Операционная система UNIX является особенно уязвимой

Российская Федерация

Подлинный текст на русском языке
9 июня 1999 г.

Общие положения

1. Одна из характерных особенностей современного этапа мирового научно-технического прогресса связана с глобальной информационной революцией — стремительным развитием и повсеместным внедрением новейших информационных технологий и глобальных средств телекоммуникации. Проникая во все сферы жизнедеятельности государств, информационная революция расширяет возможности развития международного сотрудничества, формирует глобальное информационное пространство, в котором информация приобретает свойства ценнейшего элемента национального достояния, его стратегического ресурса.

2. Вместе с тем становится очевидным, что наряду с положительными моментами такого процесса создается и реальная угроза использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности и безопасности, соблюдения принципов суверенного равенства государств, мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека.

3. Увеличение за счет новейших информационных технологий военного потенциала стран ведет к изменению глобального и регионального балансов сил, возникновению напряженности между традиционными и нарождающимися центрами силы и влияния.

4. Формируется принципиально новая сфера противоборства на международной арене, создается риск нового витка гонки вооружений на основе научно-технических достижений в области информатизации и связи. При этом затрагивается как сфера национальной безопасности отдельных государств, так и общая система международной коллективной безопасности на региональных и глобальном уровнях.

5. Речь идет о создании информационного оружия, применение которого с учетом уровня информатизации общества и уязвимости критически важных структур может иметь разрушительные последствия, сравнимые с воздействием оружия массового поражения. Очевидно, что таким оружием могут воспользоваться и террористические, экстремистские или криминальные группы, а также отдельные правонарушители.

6. Таким образом, универсальность, скрытность или обезличенность, возможность широкого трансграничного применения, экономичность и общая эффективность делают информационное оружие чрезвычайно опасным средством воздействия, причем разработка и применение такого оружия практически не регулируются нормами современного международного права.

7. В этой связи возникает очевидная потребность в международно-правовом регулировании мировых процессов гражданской и военной информатизации, разработке отвечающей интересам мировой безопасности согласованной международной платформы по проблеме информационной безопасности.

Предлагаемая модель действий

8. Основой дальнейших усилий международного сообщества в этом направлении может стать принятая консенсусом резолюция 53/70 Генеральной Ассамблеи от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», проект которой был инициативно внесен Российской Федерацией.

9. В дальнейшем следует вести дело к принятию Генеральной Ассамблеей резолюций по проблеме информационной безопасности, конкретизированных в части ограничения угроз как террористического или криминального, так и военного характера.

10. Необходимо продолжать совместное рассмотрение ситуации в сфере информационной безопасности с целью выявления всех имеющихся позиций и взглядов и их учета в дальнейшем общем продвижении идеи.

11. По мере определения общих подходов и тенденций вести дело к разработке международных принципов (режима, кодекса поведения государств), направленных на укрепление международной информационной безопасности, которые могли бы быть первоначально сформулированы в виде многосторонней декларации, а в перспективе закреплены в форме многостороннего международно-правового документа. Проработку этих вопросов целесообразно вести также в рамках Женевской конференции по разоружению.

12. При этом следует исходить из необходимости рассмотрения и принятия международным сообществом упомянутых принципов в комплексе, т.е. с учетом угроз военного, террористического или криминального характера и применительно как к военным, так и к гражданским сферам.

Основные угрозы в сфере международной информационной безопасности

13. К числу основных угроз в сфере международной информационной безопасности относятся:

a) создание и использование средств воздействия и нанесения ущерба информационным ресурсам и системам другого государства;

b) целенаправленное информационное воздействие на критически важные структуры другого государства;

c) информационное воздействие с целью подрыва политической и социальной системы государства, психологическая обработка населения с целью дестабилизации общества;

d) действия государств, ведущие к их доминированию и контролю в информационном пространстве, противодействие доступу к новейшим информационным технологиям, создание условий технологической зависимости в сфере информатизации в ущерб другим государствам;

e) действия международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющие угрозу информационным ресурсам и критически важным структурам государств;

f) разработка и принятие государствами планов, доктрин, предусматривающих возможность ведения информационных войн и способных спровоцировать гонку вооружений, а также вызвать напряженность в отношениях между государствами и собственно возникновение информационных войн;

g) использование информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере;

h) неконтролируемое трансграничное распространение информации, противоречащее принципам и нормам международного права, а также внутреннему законодательству конкретных стран;

i) манипулирование информационными потоками, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этнических и эстетических ценностей;

j) информационная экспансия, приобретение монопольного контроля над национальными информационно-телекоммуникационными инфраструктурами другого государства, включая условия их функционирования в международном информационном пространстве.

Основные задачи и цели разработки режима международной информационной безопасности

14. Существует необходимость в формировании международно-правовой основы для:

a) определения признаков и классификации информационных войн;
b) определения признаков и классификации информационного оружия, а также методов и средств, которые можно отнести к информационному оружию;
c) ограничения оборота информационного оружия;
d) запрещения разработки, распространения и применения особо опасных видов информационного оружия;
e) предотвращения угрозы возникновения информационных войн;
f) запрещения использования информационных технологий и средств во враждебных целях и, в частности, против согласованных категорий объектов;
g) признания сравнимости применения информационного оружия в отношении критически важных структур с последствиями применения оружия массового поражения;
h) создания условий равноправного и безопасного международного информационного обмена на основе баланса интересов личности, общества и государства;
i) предотвращения угроз использования информационных технологий и средств в террористических и других преступных целях;
j) предотвращения угрозы использования информационных технологий и средств для воздействия на общественное сознание с целью дестабилизации общества и государства;
k) разработки процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия;
l) создания механизма разрешения конфликтных ситуаций в сфере информационной безопасности;
m) создания международной системы сертификации технологий и средств информатизации (в том числе программно-технических) в части гарантий их информационной безопасности;
n) развития системы международного взаимодействия правоохранительных органов по предотвращению преступлений в информационной сфере;
o) создания механизма контроля выполнения условий режима международной информационной безопасности;
p) гармонизации национальных законодательств в части обеспечения информационной безопасности.

Основные понятия, относящиеся к международной информационной безопасности

15. В число основных понятий, относящихся к международной информационной безопасности, входят:

a) информационное пространство — сфера деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, информационно-телекоммуникационную инфраструктуру и собственно информацию;
b) информационные ресурсы — информационная инфраструктура (технические средства и системы формирования, обработки, хранения и передачи информации), включая массивы и базы данных и собственно информацию и ее потоки;
c) информационная война — противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической и социальной систем другого государства, а также массированной психологической обработки населения и дестабилизации общества;
d) информационное оружие — средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам другого государства, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные системы, а также массированной психологической обработки населения с целью дестабилизации общества и государства;
e) информационная безопасность — состояние защищенности основных интересов личности, общества и государства в информационном пространстве, включая информационно-телекоммуникационную инфраструктуру и собственно информацию в отношении таких ее свойств, как целостность, объективность, доступность и конфиденциальность;
f) угроза информационной безопасности — факторы, создающие опасность основным интересам личности, общества и государства в информационном пространстве;
g) международная информационная безопасность — состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;
h) неправомерное использование информационно-телекоммуникационных систем и информационных ресурсов — использование телекоммуникационных и информационных систем и ресурсов без соответствующих прав или с нарушением соответствующих правил, законодательства или норм международного права;
i) несанкционированное вмешательство в информационно-телекоммуникационные системы и информационные ресурсы — вмешательство в процессы сбора, обработки, накопления, хранения, поиска, распространения и использования информации с целью

нарушения нормального функционирования информационных систем или нарушение целостности, конфиденциальности и доступности информационных ресурсов;

j) критически важные структуры — объекты, системы и институты государства, целенаправленное воздействие на информационные ресурсы которых может иметь последствия, прямо затрагивающие национальную безопасность (транспорт, энергоснабжение, кредитно-финансовая сфера, связь, органы государственного управления, системы обороны, правоохранительные органы, стратегические информационные ресурсы, научные объекты и научно-технические разработки, объекты повышенной технической и экологической опасности, органы ликвидации последствий стихийных бедствий и иных чрезвычайных ситуаций);

k) международный информационный терроризм — использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в террористических целях;

l) международная информационная преступность — использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в противоправных целях.

Саудовская Аравия

Подлинный текст на арабском языке
27 мая 1999 г.

Во всех государствах, которые все более широко используют электронные информационные системы, многие правительственные и частные учреждения добились прогресса в области информационной технологии. Тем не менее по мере ускорения такого прогресса возрастает и число актов, направленных на нарушение функционирования таких информационных систем, их дестабилизацию и вмешательство в них, которые предпринимаются различными образованиями в преступных и террористических целях. Эта деятельность наносит ущерб экономике и обществу и подрывает безопасность. Весьма важное значение имеет внедрение международных принципов и норм, с тем чтобы противостоять угрозам информационной безопасности и попыткам нарушения такой безопасности, а также с тем чтобы бороться с такими международными актами и в уголовном порядке наказывать виновных в них. Соответствующие международные организации должны обеспечивать, чтобы те, кто повинен в совершении таких актов, представали перед правосудием и несли наказание.

Соединенное Королевство Великобритании и Северной Ирландии

Подлинный текст на английском языке

30 мая 1999 г.

Общие положения

1. Связь между информационными системами во всем мире в настоящее время достигла такой степени, что многие, если не все, государства стоят перед лицом потенциальной опасности того, что жизненно важные элементы их инфраструктуры подвергнутся электронному нападению со стороны преступников и террористов. Хотя опасность такого электронного нападения, вероятно, в настоящее время невелика, она будет возрастать в будущем по мере того, как государственный и частный сектора будут все более широко использовать компьютерные системы, которые будут во все большей степени связаны друг с другом. Кроме того, поскольку такие системы связаны друг с другом в международном масштабе, данная угроза имеет трансграничный характер. Поэтому попытки преступников и террористов проникнуть в наши системы со злым умыслом представляют собой проблему для всех членов Организации Объединенных Наций. В связи с этим Соединенное Королевство Великобритании и Северной Ирландии приветствует шаги, направленные на изучение соответствующих средств борьбы как на односторонней, так и на многосторонней основе, с помощью которых мы могли бы обеспечить неприкосновенность от таких нападений основанной на информационных системах жизненно важной инфраструктуры.

Меры на национальном уровне

2. В этих целях в январе 1999 г. правительство Ее Величества объявило о шагах, призванных свести к минимуму опасность электронного нападения на чрезвычайно важную национальную инфраструктуру Соединенного Королевства. Меры на национальном уровне включают:

a) обеспечение идентификации в рамках правительства всех чрезвычайно важных систем, а также обеспечение эффективного управления деятельностью по защите таких систем и соответствующей проверки;

b) разработка в сотрудничестве с частным сектором мер, которые будут соответствовать уровню опасности, и обеспечение адекватных стандартов защиты ключевых систем, охватываемых жизненно важной национальной инфраструктурой;

c) повышение уровня информированности и стандартов в области информационной безопасности в частном секторе в целом путем дальнейшей реализации уже существующих инициатив, нацеленных на внедрение и применение наилучших практических методов в этой области.

Меры на международном уровне

3. В то же время тот факт, что связь между информационными системами носит трансграничный характер, означает, что нападения на системы в других государствах могут оказать негативное воздействие и на жизненно важную национальную инфраструктуру самого Соединенного Королевства и что террористы и преступники, действующие в той или иной третьей стране, могут попытаться напасть на системы в Соединенном Королевстве. Поэтому Соединенное Королевство признает важное значение международного сотрудничества в деле борьбы с угрозой преступного нападения и рассчитывает на расширение уже проводимых в настоящее время диалогов со своими международными партнерами по данным проблемам. Эта деятельность включает в себя работу Группы «большой восьмерки» по вопросам преступности в области высоких технологий, которая касается правовой взаимопомощи, а также работу, проводимую в Совете Европы в связи с разработкой конвенции о кибернетической преступности.

4. Соединенное Королевство полагает, что Организации Объединенных Наций следует следить за ходом работы в рамках этих и других форумов в целях определения в будущем тех видов мероприятий, касающихся вопросов существа, которые она могла бы с пользой осуществлять в этой области. В их число могли бы входить разработка международных принципов в целях укрепления безопасности глобальных систем и содействия борьбе с международным информационным терроризмом и преступностью.

Соединенные Штаты Америки

Подлинный текст на английском языке
20 мая 1999 г.

Общий обзор проблем в области информационной безопасности и определение основных понятий

1. Соединенные Штаты Америки полагают, что информационная безопасность представляет собой широкую и сложную тему, охватывающую многие факторы и затрагивающую многие разнообразные виды деятельности отдельных лиц, групп и правительств. Хотя эта общая тема включает в себя аспекты, которые связаны с международным миром и безопасностью (работа Первого комитета), она также охватывает технические аспекты, которые касаются глобальных коммуникационных систем, равно как и нетехнические вопросы, связанные с экономическим сотрудничеством и торговлей, правами интеллектуальной собственности, соблюдением законности, сотрудничеством в борьбе с терроризмом и другими проблемами, рассматриваемыми в рамках Второго или Шестого

комитета. Меры и программы правительств ни в коей степени не являются единственными надлежащими инструментами, поскольку информационная безопасность также затрагивает важные проблемы, представляющие интерес для отдельных лиц, ассоциаций, предприятий и других организаций, действующих в частном секторе.

Аспекты, касающиеся международной безопасности

2. В периоды вооруженных конфликтов государства используют различные методы, связанные с информационной безопасностью. Двумя распространенными примерами являются создание радиопомех на определенных частотах и использование электромагнитных импульсов для борьбы с противником; такие методы далеко не новы. В будущем для вооруженных сил того или иного государства важное значение будет иметь защита их собственных сетей передачи данных и других основанных на применении компьютеров систем. Кроме этого, государствам-членам необходимо располагать потенциалом для восстановления ключевых информационных систем в тех случаях, когда стихийное бедствие или имеющая катастрофические последствия чрезвычайная ситуация выводит из строя ключевые объекты коммуникации или другие сети передачи данных в государственном и частном секторах. Информационная безопасность охватывает также защиту данных, связанных с военным потенциалом и другими аспектами национальной безопасности.

Экономические, торговые и технические факторы

3. Концепция информационной безопасности предполагает необходимость в защите результатов научных исследований коммерческого характера, а также производственных технологий и других видов конфиденциальных данных (например, планы маркетинга и информация служб, работающих с клиентурой).

4. Информационная безопасность связана также с необходимостью обеспечения соблюдения международных соглашений об интеллектуальной собственности (такой как видео- и аудиоматериалы, а также компьютерное программное обеспечение), с тем чтобы защитить ее от несанкционированного копирования и продажи. Защита информации и данных частного характера представляет собой еще один аспект информационной безопасности и связана с обеспечением безопасности информации личного и коммерческого характера, передаваемой через общественные международные сети связи или частные системы передачи данных.

5. Что касается технических аспектов, то положения, применяемые Международным союзом электросвязи, и мероприятия аналогичных национальных учреждений обеспечивают совместимость электронных сигналов, надлежащее применение электромагнитного спектра и надежность международной сети связи в целом. Эти функции выполняют также и космические спутники, которые обеспечивают оказание широкого комплекса услуг, таких как передача речевой корреспонденции и данных, а также данных локаторов и другой информации, используемой в авиации и мореплавании, а также при проведении исследований и спасательных операций. Кроме этого, соответствующие стандарты в области проектирования и безопасности обеспечивают чрезвычайно важные гарантии производителям и пользователям электронных устройств, включая компьютеры. Все эти регулятивные и административные функции можно ассоциировать с широкой концепцией информационной безопасности.

Обеспечение соблюдения законов и сотрудничество в борьбе с терроризмом
6. Широкомасштабное применение информационных технологий породило беспрецедентно высокий уровень глобальной взаимозависимости и взаимосвязи информационных систем, в результате чего многие аспекты национальной и международной деятельности, в рамках как государственного, так и частного секторов, теоретически могут оказаться под угрозой нападения со стороны преступников или террористов.

7. Хотя степень применения информационных технологий в разных государствах может быть различной, масштабы деятельности, которая связана с применением таких средств коммуникации (экономическая, торговая, промышленная, юридическая деятельность, а также деятельность в области образования) позволяют предположить, что потенциально все государства могут столкнуться с последствиями деятельности различных преступников. Кроме этого, следует ожидать, что применение информационных технологий будет по-прежнему расширяться, поскольку эти технологии будут играть все более важную роль для стабильного функционирования правительств, а также для поддержания ключевых глобальных коммерческих и коммуникационных систем, обеспечивающих взаимодействие между государствами.

8. Поэтому Соединенные Штаты рассматривают потенциальную опасность использования преступниками информационных технологий как проблему, представляющую интерес для всех государств, и разделяют выраженное другими странами мнение о том, что нам необходимо в одностороннем и многостороннем порядке содействовать внедрению надлежащих мер для

обеспечения неприкосновенности наших ресурсов, использование которых зависит от применения информационных технологий.

9. Соединенные Штаты также полагают, что любое незаконное вмешательство или попытка нарушить или изменить любой аспект их национальных информационных систем представляют собой потенциальную опасность для основных объектов их национальной инфраструктуры, а значит, и угрозу их национальным интересам. Соединенные Штаты, признавая потенциальную серьезность такой угрозы, выступили инициатором реализации на национальном уровне долгосрочных программ в государственном и частном секторах, которые рассчитаны на обеспечение защиты чрезвычайно важных объектов их национальной инфраструктуры. Тем не менее Соединенные Штаты признают также, что в контексте все большей глобальной взаимозависимости многих этих весьма важных инфраструктур успех их усилий на национальном уровне, предпринимаемых для защиты своих информационно-коммуникационных систем, в конечном счете будет отчасти зависеть от степени обеспечения безопасности тех находящихся за пределами Соединенных Штатов систем, с которыми они связаны.

10. Поэтому Соединенные Штаты полагают, что всем государствам следует принять на национальном уровне меры, необходимые как для обеспечения охраны их национальных информационных систем, так и для обеспечения того, чтобы преступники или международные террористы, действующие на их национальной территории, которые пытаются нарушить функционирование этих систем, карались за это по всей строгости закона. Каждое государство должно принять меры для того, чтобы его информационные системы были надежны и обеспечены как можно более надежными системами защиты на случай возможных попыток со стороны преступников использовать системы в своих целях или блокировать их работу, а также обеспечить быструю восстанавливаемость информационных систем в случае сбоев в их работе.

11. Уголовное право Соединенных Штатов запрещает вмешиваться в информационные инфраструктуры Соединенных Штатов Америки. Соединенные Штаты настоятельно призывают все государства провести обзор своих соответствующих национальных законов, с тем чтобы обеспечить включение в них надлежащих положений, касающихся преследования виновных в действиях, связанных с использованием информационных систем в преступных или террористических целях. Соединенные Штаты считают необходимым внесение на постоянной основе поправок в свои законы, касающиеся компьютерных сетей, с тем

чтобы совершенствовать их и приводить их в соответствие с реалиями, порождаемыми новыми проблемами.

Целесообразность разработки международных принципов

12. Как указывалось выше, информационная безопасность представляет собой широкую и сложную тему. Она имеет много измерений, которые чрезвычайно сложно переплетены между собой. Учитывая несомненную необходимость в анализе всех аспектов информационной безопасности и в достижении четкого понимания того, как эти аспекты взаимодействуют, было бы преждевременно приступать к разработке всеобъемлющих принципов, касающихся информационной безопасности во всех ее аспектах. Вместо этого международному сообществу следует проделать значительную работу с тем, чтобы на систематической основе осмыслить пройденный этап, прежде чем двигаться дальше. В целях содействия этому государствам-членам необходимо стремиться к ознакомлению с идеями и мнениями широкого круга экспертов в наших соответствующих правительствах и странах.

13. Тем не менее уже очевидно, что международное сотрудничество имеет важное значение в деле эффективного решения новых и сложных проблем, порождаемых информационным терроризмом и преступными элементами. В настоящее время проводится несколько многосторонних мероприятий, касающихся проблем международного сотрудничества. Совет Европы изучает проект конвенции о кибернетической преступности; Группа по вопросам преступности в области высоких технологий «большой восьмерки» изучает меры по оказанию взаимопомощи в правовой области, а также смежные проблемы, связанные с преступностью в области высоких технологий; Организация американских государств также учредила группу для изучения этих проблем; Азиатский и дальневосточный институт Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями изучает смежные вопросы в рамках Организации Объединенных Наций.

14. Все эти прилагаемые в настоящее время усилия заслуживают высокой оценки, и их, несомненно, необходимо и далее активизировать, с тем чтобы они могли принести свои плоды. Было бы весьма недальновидно, если бы Генеральная Ассамблея занялась разработкой стратегий или конкретных мероприятий, которые могли бы нанести ущерб уже проводимой международным сообществом соответствующей работе или стать ей помехой.

Источник: Док. Генеральной Ассамблеи ООН A/54/213, 10 августа 1999.

Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности

Доклад Генерального секретаря[12]

Содержание

I. Введение

1. В пунктах 2 и 3 своей резолюции 54/49 от 1 декабря 1999 г., озаглавленной «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», Генеральная Ассамблея просила все государства-члены информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам: a) общая оценка проблем информационной безопасности; b) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов; и c) целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и криминалом, а также просила Генерального секретаря представить доклад Генеральной Ассамблее на ее пятьдесят пятой сессии.

2. 14 марта 2000 г. Генеральный секретарь направил государствам-членам вербальную ноту с просьбой представить их мнения в ответ на просьбу Ассамблеи. Ответы, полученные от правительств на сегодняшний день, воспроизводятся в главе II настоящего доклада. Любые другие поступающие ответы будут издаваться в качестве добавлений к настоящему докладу.

II. Ответы, полученные от правительств

Иордания

Подлинный текст на арабском языке
16 мая 2000 г.

1. Применение информационно-технологических систем привело к положительным результатам для международного сообщества в плане

[12]Настоящий доклад подготовлен на основе материалов, представленных государствами-членами.

поддержания стабильности и безопасности, однако злоупотребления этими новыми достижениями и методами:
a) облегчат организацию террористических сетей, элементы которых разбросаны по весьма широким географическим пространствам, с учетом возможностей быстрой связи;
b) затруднят контроль за современными средствами связи с учетом быстро возникающих технологических сложностей и существования в большинстве стран законов, ограничивающих вмешательство в свободу коммуникации, которой пользуются все люди.

2. С учетом нашей приверженности делу принятия надлежащих мер и в качестве мер предосторожности против террористической деятельности мы рекомендуем следующее:
a) разработать специальное чрезвычайное законодательство, с тем чтобы позволять службам безопасности получать доступ в центры управления компаниями, связанными с передовыми системами, и частично контролировать их;
b) координировать вместе с компаниями и ведомствами, занимающимися обеспечением связи, усилия по подготовке специалистов из служб безопасности для работы с такими системами в периоды кризисов;
c) оказывать поддержку сектору информационной технологии и техники связи и связанным с ним концепциям безопасности, а также обеспечивать инфраструктуру и надлежащую подготовку для содействия поддержанию международного мира и безопасности.

Катар

Подлинный текст на арабском языке
17 мая 2000 г.

1. Шпионаж: предотвращение доступа неуполномоченной стороны к содержанию глобальных информационных и телекоммуникационных систем.

2. Саботаж: предотвращение частичного или полного уничтожения глобальных информационных и телекоммуникационных систем.

3. Регистрация: регистрация информации, направленной через глобальные информационные системы или телекоммуникационные системы, включая интеллектуальную собственность.

4. Подделка: предотвращение подделки информации, направляемой через глобальные информационные и телекоммуникационные системы.

5. Защита: разработка мер по электронной защите информации, направляемой через глобальные информационные и телекоммуникационные системы.

6. Законодательство: разработка необходимых законов в отношении всех электронных операций в целях обеспечения прав участников и наказания правонарушителей.

Российская Федерация

Подлинный текст на русском языке
12 мая 2000 г.

Принципы, касающиеся международной информационной безопасности
Использование терминов

Для целей настоящих принципов применяются следующие термины
1. Информационное пространство — сфера деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, информационно-телекоммуникационную инфраструктуру и собственную информацию.

2. Информационные ресурсы — информационная инфраструктура (технические средства и системы формирования, обработки, хранения и передачи информации), включая массивы и базы данных и собственную информацию и ее потоки.

3. Информационная война — противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической, экономической и социальной систем, а также массированной психологической обработки населения с целью дестабилизации общества и государства.

4. Информационное оружие — средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам государства, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные системы государства, а также массированной психологической обработки населения с целью дестабилизации общества и государства.

5. Информационная безопасность — состояние защищенности основных интересов личности, общества и государства в информационном

пространстве, включая информационно-телекоммуникационную инфраструктуру и собственно информацию в отношении таких ее свойств, как целостность, объективность, доступность и конфиденциальность.

6. Угроза информационной безопасности — факторы, создающие опасность основным интересам личности, общества и государства в информационном пространстве.

7. Международная информационная безопасность — состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

8. Неправомерное использование ннформационно-телекоммуникационных систем и информационных ресурсов — использование телекоммуникационных и информационных систем и ресурсов без соответствующих прав или с нарушением установленных правил, законодательства или норм международного права.

9. Несанкционированное вмешательство в информационно-телекоммуникацнонные системы и информационные ресурсы — вмешательство в процессы сбора, обработки, накопления, хранения, отображения, поиска, распространения и использования информации с целью нарушения нормального функционирования информационных систем или нарушение целостности, конфиденциальности и доступности информационных ресурсов.

10. Критически важные структуры — объекты, системы и институты государства, целенаправленное воздействие на информационные ресурсы которых может иметь последствия, прямо затрагивающие национальную безопасность (транспорт, энергоснабжение, кредитно-финансовая сфера, связь, органы государственного управления, система обороны, правоохранительные органы, стратегические информационные ресурсы, научные объекты и научно-технические разработки, объекты повышенной технической и экологической опасности, органы ликвидации последствий стихийных бедствий и иных чрезвычайных ситуаций).

11. Международный информационный терроризм — использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в террористических целях.

12. Международная информационная преступность — использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в противоправных целях.

Принцип 1

1. Деятельность каждого государства и других субъектов международного права в международном информационном пространстве должна способствовать общему социальному и экономическому развитию и осуществляться таким образом, чтобы быть совместимой с задачами поддержания мировой стабильности и безопасности, суверенными правами других государств, интересами безопасности, принципами мирного урегулирования споров и конфликтов, неприменение силы, невмешательства во внутренние дела, уважения прав и свобод человека.

2. Такая деятельность также должна быть совместимой с правом каждого искать, получать и распространять информацию и идеи, как это зафиксировано в соответствующих документах Организации Объединенных Наций, с учетом того, что такое право может быть ограничено законом в целях защиты интересов безопасности каждого государства.

3. При этом каждое государство и другие субъекты международного права должны иметь равные права на защиту своих информационных ресурсов и критически важных структур от неправомерного использования и несанкционированного информационного вмешательства и могут рассчитывать на поддержку мирового сообщества в реализации этих прав.

Принцип II

Государства будут стремиться к ограничению угроз в сфере международной информационной безопасности и с этой целью воздерживаться от:

a) разработки, создания и использования средств воздействия и нанесения ущерба информационным ресурсам и системам другого государства;

b) целенаправленного информационного воздействия на критически важные структуры другого государства;

c) информационного воздействия с целью подрыва политической, экономической и социальной системы других государств, психологической обработки населения с целью дестабилизации общества;

d) несанкционированного вмешательства в информационно-телекоммуникационные системы и информационные ресурсы, а также их неправомерного использования;

e) действий, ведущих к доминированию и контролю в информационном пространстве;
f) противодействия доступу к новейшим информационным технологиям, создания условий технологической зависимости в сфере информатизации в ущерб другим государствам;
g) поощрения действий международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющих угрозу информационным ресурсам и критически важным структурам государств;
h) разработки и принятия планов, доктрин, предусматривающих возможность ведения информационных войн и способных спровоцировать гонку вооружений, а также вызвать напряженность в отношениях между государствами и собственно возникновение информационных войн;
i) использования информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере;
j) трансграничного распространения информации, противоречащей принципам и нормам международного права, а также внутреннему законодательству конкретных стран;
k) манипулирования информационными потоками, дезинформации и сокрытия информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этических и эстетических ценностей;
l) информационной экспансии, приобретения контроля над национальными информационно-телекоммуникационными инфраструктурами другого государства, включая условия их функционирования в международном информационном пространстве.

Принцип III
Организация Объединенных Наций и соответствующие учреждения системы Организации Объединенных Наций будут содействовать международному сотрудничеству, целью которого является ограничение угроз в сфере международной информационной безопасности, и формированию с этой целью международно-правовой основы для:
a) определения признаков и классификации информационных войн;
b) определения признаков и классификации информационного оружия и средств, которые можно отнести к информационному оружию;
c) ограничения оборота информационного оружия;
d) запрещения разработки, распространения и применения информационного оружия;

e) предотвращения угрозы возникновения информационных войн;
f) признания опасности применения информационного оружия в отношении критически важных структур, сравнимой с опасностью применения оружия массового поражения;
g) создания условий для равноправного и безопасного международного информационного обмена на основе общепризнанных норм и принципов международного права;
h) предотвращения использования информационных технологий и средств в террористических и других преступных целях;
i) предотвращения использования информационных технологий и средств для воздействия на общественное сознание с целью дестабилизации общества и государства;
j) разработки процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия;
k) создания системы международного мониторинга для отслеживания угроз, проявляющихся в информационной сфере;
1) создания механизма контроля выполнения условий режима международной информационной безопасности;
m) создания механизма разрешения конфликтных ситуаций в сфере информационной безопасности;
n) создания международной системы сертификации технологий и средств информатизации и телекоммуникации (в том числе программно-технических) в части гарантий их информационной безопасности;
o) развития системы международного взаимодействия правоохранительных органов по предотвращению и пресечению правонарушений в информационном пространстве;
p) гармонизации на основе добровольности национального законодательства в части обеспечения информационной безопасности.

Принцип IV
Государства и другие субъекты международного права должны нести международную ответственность за деятельность в информационном пространстве, осуществляемую ими, под их юрисдикцией или в рамках международных организаций, членами которой они являются, и за соответствие любой такой деятельности принципам, содержащимся в настоящем документе.

Принцип V
Любой спор между государствами и другими субъектами международного права, возникающий из применения настоящих принципов, разрешается с помощью установленных процедур мирного урегулирования споров.

Польша

Подлинный текст на английском языке
8 сентября 2000 г.

Общая оценка проблем информационной безопасности и определение основных понятий

1. Информационно-телекоммуникационные технологии в значительной степени облегчают свободный поток информации и приносят огромные выгоды как отдельным лицам, так и деловым кругам и правительствам по всему миру. Они способствуют развитию демократии и свободы слова, а также продвижению вперед гражданского общества. Польша считает важным поощрять и обеспечивать дальнейшее развитие информационно-телекоммуникационных технологий, равно как и укреплять принцип свободы информации и свободного выбора и использования технических средств ее передачи.

2. Польша признает наличие потенциальной угрозы несанкционированного вмешательства или неправомерного использования информационно-телекоммуникационных систем, целостности критически важных информационных инфраструктур и информационных ресурсов отдельных лиц, предприятий, учебных или медицинских учреждений и других организаций частного сектора, а также правительств. Информационная безопасность, охватывающая широкий спектр вопросов, связанных с безопасностью информационно-телекоммуникационных систем, требует защиты в плане доступа, конфиденциальности, наличия и целостности информации, обрабатываемой такими системами. Информационная безопасность распространяется также на защиту информации, касающейся военного потенциала и других аспектов национальной безопасности. Недостаточная защита информационных ресурсов и информационно-телекоммуникационных систем, которые имеют жизненно важное значение с точки зрения интересов соответствующих государств, также может представлять собой угрозу международной безопасности.

3. Вместе с тем Польша считает, что существующие угрозы носят трансграничный характер и что технические средства, позволяющие наносить ущерб информационно-телекоммуникационным системам, являются общедоступными. Одновременно, в своей основе их нельзя классифицировать как исключительно гражданские или военные. Такие угрозы связаны главным образом с использованием таких систем отдельными лицами или террористическими организациями в преступных целях и как таковые не могут быть сдержаны традиционными соглашениями в области контроля над вооружениями, поскольку последние могут

ограничивать или сдерживать свободный поток информации и использование информационной технологии в мирных целях, от чего зависит экономика всех стран мира. Любые превентивные действия, направленные на сдерживание потенциальных преступных или террористических действий, включая угрозы международному миру, должны быть сконцентрированы на защите информационных ресурсов и информационных систем.

4. Для защиты целостности базирующихся на использовании информации критически важных структур и информационных ресурсов и с тем чтобы противостоять угрозам, которым подвергается информационная безопасность, Польша выступает за эффективное и всестороннее международное сотрудничество в правовой области, а также за строгое применение действующих внутренних законов и, при необходимости, разработку новых законодательных актов.

Действия на национальном уровне

5. Каждая страна имеет право и обязана защищать свою собственную информацию и информационные системы. С этой целью Польша разработала следующие правовые положения:

a) Закон о защите секретной информации от 22 января 1999 г., в котором устанавливаются правила обеспечения вышеупомянутой защиты;

b) Закон о защите частной информации от 29 октября 1997 г., который регулирует правила поведения в области обработки данных, а также права лиц, информация о которых подлежит обработке;

c) Уголовно-процессуальный кодекс от 6 июня 1997 г., в котором устанавливается уголовная ответственность не только за традиционные виды преступлений, направленных против мер по защите информации, — передача секретной и закрытой информации, — но и за уничтожение или изъятие компьютерных данных или нанесение ущерба или внесение в них изменений, а также за вмешательство в процессы автоматизированного накопления или передачи информации, касающейся вопросов национальной обороны, безопасности коммуникационных систем и функционирования органов государственной власти.

Целесообразность разработки международных принципов и мер

6. Огромные достижения в области информационно-телекоммуникационных технологий требуют дальнейшего развития международного права с целью укрепления информационной безопасности. Вопросы преступного использования информации, включая правовые аспекты, были одними из основных тем десятого Конгресса Организации Объединенных Наций по предупреждению преступности и

обращению с правонарушителями, который состоялся 10-17 апреля 2000 г. (см.: A/CONF.187/15), и Польша признает руководящую роль Комиссии Организации Объединенных Наций по предупреждению преступности и уголовному правосудию в деле разработки международных принципов информационной безопасности и возможных методов и способов действий, которые бы обеспечили соблюдение необходимого баланса между правом личности на частную жизнь и обязанностями различных ветвей власти. Этот форум также содействует и способствует координации деятельности межрегиональных и региональных учреждений по предупреждению преступности и обращению с правонарушителями.

7. Одновременно Польша осуществляет также активное межправительственное сотрудничество (с Германией соглашение заключено; с Венгрией, Словакией, Украиной, Францией и Эстонией ведутся переговоры) для заключения соглашений о защите информации, особенно информации частного характера, информации, касающейся медицинских данных, прав интеллектуальной собственности или результатов научных исследований, от любого несанкционированного вмешательства или любых других преступлений, включая подделку и незаконные банковские или финансовые сделки, а также о защите информационных ресурсов и сетей от целенаправленного нанесения им ущерба.

Источник: Док. Генеральной Ассамблеи ООН A/55/140, 10 июля 2000; A/55/140/Add.1, 3 октября 2000; A/55/140/Corr.1, 3 октября 2000.

ПРИЛОЖЕНИЕ 5. СОВМЕСТНОЕ ЗАЯВЛЕНИЕ ОБ ОБЩИХ ВЫЗОВАХ БЕЗОПАСНОСТИ НА РУБЕЖЕ XXI ВЕКА

Мы, Президенты Российской Федерации и Соединенных Штатов Америки, заявляем, что сотрудничество между Россией и США будет иметь в XXI веке чрезвычайно важное значение для содействия процветанию и укрепления безопасности во всем мире. В этой связи мы подтверждаем, что Российская Федерация и Соединенные Штаты Америки являются естественными партнерами в обеспечении международного мира и стабильности. Мы уделили особое внимание наращиванию совместных усилий в деле ликвидации угроз, унаследованных от времен «холодной войны», а также отражения общих вызовов безопасности на рубеже XXI века.

Мы считаем, что самую серьезную и насущную опасность представляет распространение ядерного, биологического, химического и других видов оружия массового уничтожения, технологий его производства и средств доставки. В условиях возрастающей взаимозависимости современного мира эти угрозы обретают транснациональный и глобальный характер, затрагивая не только национальную безопасность Российской Федерации и Соединенных Штатов, но и международную стабильность в целом. Вновь подтверждаем решимость России и США активно и тесно сотрудничать друг с другом, а также со всеми другими заинтересованными государствами с целью предотвращения и уменьшения такой угрозы посредством осуществления новых шагов, поиска новых форм взаимодействия и укрепления общепризнанных международных норм. Мы признаем, что должно быть сделано больше, и сегодня мы предприняли ряд шагов по укреплению не только нашей безопасности, но и глобальной безопасности. Мы заявляем о своей твердой приверженности активизации переговоров по скорейшему завершению работы над Протоколом к Конвенции о запрещении биологического оружия. Мы приступаем к сотрудничеству на новом и важном направлении, каковым является дальнейшее уменьшение риска ложных предупреждений о ракетном нападении. И мы договорились о принципах, которые будут регулировать наше сотрудничество по обращению и утилизации плутония, изъятого из ядерных оружейных программ, с тем чтобы его никогда нельзя было вновь использовать в ядерном оружии. Общие обязательства сделали Россию и США партнерами в разработке основ международного режима нераспространения, включая Договор о нераспространении ядерного оружия, гарантии МАГАТЭ, Конвенцию о запрещении биологического и токсинного оружия и Договор о всеобъемлющем запрещении ядерных

испытаний. Россия и США подтверждают свою приверженность цели присоединения всех стран к Договору о нераспространении ядерного оружия в его нынешнем виде, без изменений. Они также привержены более строгим правилам Группы ядерных поставщиков. Участвуя в Конференции по разоружению, наши государства вместе добились успеха в переговорах по выработке Конвенции о запрещении химического оружия и Договора о всеобъемлющем запрещении ядерных испытаний и призывают все страны присоединиться к этим договорам. Руководствуясь этими обязательствами, они предприняли существенные практические шаги по уменьшению глобальной ядерной угрозы и обеспечению контроля за передачей чувствительной технологии. Россия и США продолжают испытывать глубокую озабоченность по поводу ядерных испытаний в Южной Азии и подтверждают свою приверженность тесной координации в деле поддержки всех шагов, изложенных в Совместном коммюнике «пятерки», как они одобрены «восьмеркой» и Советом Безопасности ООН.

Договор о СНВ и инициативы Президентов в области сокращения ядерных вооружений, предпринятые в 1991-1992 гг., помогут России и США обеспечить достижение их конечной цели ядерного разоружения и укрепление международной безопасности. Мы вместе ликвидировали более 1 700 тяжелых бомбардировщиков и пусковых установок ракет, включая более чем 700 шахтных установок, 45 подводных лодок, способных нести ядерные ракеты, деактивировали или ликвидировали более 18 000 стратегических и тактических ядерных боеголовок. Подтверждая приверженность строгому соблюдению своих обязательств по Договорам о СНВ и по ПРО, мы заявляем о решимости сотрудничать в деле ускорения вступления в силу Договора СНВ-2. Россия и США приступят к переговорам по более низким уровням в рамках Договора СНВ-3 сразу же после ратификации Россией Договора СНВ-2.

Россия и Соединенные Штаты в результате значительных сокращений в их ядерных силах располагают обширными запасами ядерных материалов, которые более не являются необходимыми для целей обороны. Они остаются приверженными тому, чтобы этим и другим запасам оружейных расщепляющихся материалов была обеспечена максимальная степень безопасности и учета, и подтверждают важность осуществления Соглашения о научно-техническом сотрудничестве в области обращения с плутонием, изъятым из ядерных военных программ, заключенного в июле 1998 года Председателем Правительства Российской Федерации и Вице-президентом США. Мы подтверждаем нашу приверженность дальнейшему развитию сотрудничества по

экспортному контролю как существенно важной части обеспечения нераспространения. Наши Правительства недавно создали дополнительный механизм сотрудничества в области экспорта чувствительной технологии. С этой целью на нашей сегодняшней встрече мы договорились учредить экспертные группы по ядерным вопросам, ракетной и космической технологии, всеобъемлющему и внутрифирменному контролю, контролю за передачей обычных вооружений, равно как и по правоприменению, таможенным вопросам и лицензированию с тем, чтобы укреплять сотрудничество и осуществлять конкретные проекты двустороннего взаимодействия и взаимной помощи. Эти группы будут сформированы в течение ближайшего месяца и безотлагательно начнут свою практическую деятельность. Установлен также защищенный канал связи между старшими должностными лицами обеих стран, что обеспечит быстрый и конфиденциальный обмен информацией по вопросам нераспространения. Мы вновь подтвердили важность Договора об обычных вооруженных силах в Европе (ДОВСЕ) и его фундаментальный вклад в стабильность, предсказуемость и сотрудничество в Европе. В нашей совместной работе, направленной на создание более интегрированной и безопасной Европы, мы привержены ускорению переговоров, целью которых является адаптация Договора с учетом меняющихся обстоятельств. Мы полагаем необходимым завершить работу по адаптации в самое ближайшее время. Мы подтверждаем свою приверженность соблюдению положений Договора в процессе его адаптации.

Россия и США сохраняют приверженность совместному строительству прочного мира, основанного на принципах демократии н неделимости безопасности. Они подтверждают общую цель укрепления безопасности и стабильности в интересах всех стран, а также борьбы с агрессивным национализмом и предотвращения нарушения прав человека. Они будут консультироваться и стремиться к сотрудничеству в деле предупреждения и урегулирования конфликтов, а также управления кризисами. В этой связи мы придаем важное значение оперативному сотрудничеству между вооруженными силами России и США как в двустороннем, так и многостороннем контекстах. Мы с удовлетворением отмечаем, что достигнут определенный прогресс в области оборонного сотрудничества и в особенности по укреплению ядерной безопасности и осуществлению Программы совместного уменьшения угроз.

Мы признаем, что прочность мировой финансовой и экономической системы, которая все более становится взаимозависимой, затрагивает

благосостояние людей во всех странах. Мы согласны в том, что успех экономических и структурных реформ в России имеет важное значение для международного сообщества.

Императивом защиты природных систем, от которых зависит человечество, является усиление охраны окружающей среды в XXI веке. Россия и США будут совместно работать в целях решения глобальной климатической проблемы, сохранения озонового слоя, сохранения биоразнообразия н обеспечения устойчивого использования лесов и других природных ресурсов. Мы подчеркнули необходимость углубления широкого международного и двустороннего взаимодействия в этой области.

Мы заявляем о категорической неприемлемости терроризма во всех его формах и проявлениях, независимо от мотивов. Россия и США решительно осуждают недавние террористические взрывы в Кении и Танзании. На нашей встрече сегодня мы согласовали ряд шагов, которые являются ответом на растущую угрозу терроризма.

Мы согласились активизировать совместные усилия по противодействию транснациональным угрозам экономике и безопасности наших стран, включая те из них, которые являют собой организованная преступность, незаконный оборот наркотических средств, незаконный оборот оружия, преступления с использованием компьютерной техники и других высоких технологий, легализация доходов от преступной деятельности. Мы договорились о создании двусторонней рабочей группы по правоохранительной проблематике, которая будет встречаться на регулярной основе, а также об усилении мер по исполнению законов и улучшению системы информирования общественности по вопросам ликвидации торговли женщинами и детьми. Мы согласились, что Россия и США примут активное участие в выработке эффективной конвенции ООН по борьбе с транснациональной организованной преступностью. Мы приветствуем проведение в 1999 г. в Москве встречи «восьмерки» на министерском уровне по борьбе с транснациональной преступностью.

Мы признаем важность содействия положительным сторонам и ослабления действия отрицательных сторон происходящей сейчас информационно-технологической революции, что является серьезной задачей в деле обеспечения стратегических интересов безопасности наших двух стран в будущем. В рамках усилий по решению этих проблем Россией и США уже проведены продуктивные обсуждения по

разрешению потенциальной компьютерной проблемы в 2000 г. по линии Консультативной группы по оборонным вопросам. Россия и США привержены продолжению консультаций и изучению более широких последствий данной компьютерной проблемы в целях решения вопросов, представляющих взаимный интерес и озабоченность.

Мы заявляем, что общие вызовы безопасности на рубеже XXI века могут быть отражены только посредством последовательной мобилизации усилий всего международного сообщества. Для этого должны быть использованы все имеющиеся ресурсы. В случае необходимости мировое сообщество должно своевременно принимать эффективные меры по противодействию таким угрозам. Россия и США будут продолжать играть лидирующую роль как в двустороннем, так и многостороннем планах в деле достижения общих целей в сфере безопасности.

Президент Российской Федерации	Президент Соединенных Штатов Америки

Москва, 2 сентября 1998 г.

ОБ АВТОРАХ

Алексеева Ирина Юрьевна — доктор философских наук, ведущий научный сотрудник Института философии РАН
Авчаров Иван Владимирович — МВД России
Бедрицкий Александр Владимирович — научный сотрудник Российского института стратегических исследований
Вотрин Дмитрий Сергеевич — старший советник Департамента по вопросам безопасности и разоружения МИД России
Дьяченко Владимир Александрович — доктор военных наук, профессор, Генеральный Штаб Вооруженных Сил России
Ильин Владимир Федорович — ФСБ России
Кононов Александр Анатольевич — кандидат технических наук, старший научный сотрудник Института системного анализа РАН
Крутских Андрей Владимирович — доктор исторических наук, начальник отдела Департамента по вопросам безопасности и разоружения МИД России
Мачабели Константин Ильич — МВД России
Смолян Георгий Львович — доктор философских наук, главный научный сотрудник Института системного анализа РАН
Стрельцов Анатолий Александрович — доктор технических наук, профессор, заместитель начальника управления Совета Безопасности России
Федоров Александр Валентинович — кандидат физико-математических наук, старший научный сотрудник СВР России
Черешкин Дмитрий Семенович — доктор технических наук, профессор, академик РАЕН, заведующий лабораторией Института системного анализа РАН
Цыгичко Виталий Николаевич — доктор технических наук, профессор, академик РАЕН, главный научный сотрудник Института системного анализа РАН

ИНФОРМАЦИОННЫЕ ВЫЗОВЫ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Технический редактор: К.И. Фуралева
Корректор: Т.Д. Титова

Издание ПИР-Центра политических исследований
Тел.: 335-19-55, 330-61-29, 330-61-83
Факс: 234-95-58
E-mail: info@pircenter.org
Internet: http://www.pircenter.org
Адрес: Москва, 117454, а/я 17

Подписано в печать 01.08.2001 г. Формат 60x90/16
Печать офсетная. Усл. печ.л. 20,5.
Тираж 1000 экз. Заказ № 339
Оригинал-макет и полиграфические работы —
Центр полиграфических услуг «Радуга»
ПБОЮЛ «Гайнуллин»
Лицензия: серия ИД 3 06137
Москва, Малый Могильцевский пер., 3
Тел.: 241-36-06

Отпечатано в Московской типографии № 6
Министерства РФ по делам печати, телерадиовещания и средств массовых коммуникаций
109088, Москва, Южнопортовая ул., 24