Организация Объединенных Наций A/58/373

Генеральная Ассамблея

Distr.: General
17 September 2003
Russian
Original: English/French/Russian/
Spanish

Пятьдесят восьмая сессия
Пункт 69 предварительной повестки дня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Содержание

* A/58/150.

03-52342 (R) 071003 081003

I. Введение

1. В пункте 3 своей резолюции 57/53 о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности Генеральная Ассамблея просила 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; и c) содержание соответствующих международных концепций, призванных повысить безопасность глобальных информационных и телекоммуникационных систем. В пункте 4 резолюции Генеральной Ассамблеи содержится просьба к Генеральному секретарю рассмотреть существующие и потенциальные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению, а также провести исследование концепций с помощью группы назначенных им на основе справедливого географического распределения правительственных экспертов, которая должна быть создана в 2004 году, а также при содействии государств-членов, способных оказать такое содействие, и представить доклад о результатах данного исследования Генеральной Ассамблее на ее шестидесятой сессии.

2. В вербальной ноте от 18 февраля 2003 года ко всем государствам-членам была обращена просьба информировать Генерального секретаря об их точке зрения и оценках по этому вопросу. На данный момент получено семь ответов, тексты которых воспроизводятся в разделе II ниже. Дополнительные ответы, которые поступят, будут изданы в качестве дополнения к настоящему докладу.

II. Ответы, полученные от государств-членов

Боливия

[Подлинный текст на испанском языке]
[17 июня 2003 года]

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

1. Боливия выражает свою обеспокоенность тем, что технологические достижения используются в целях, несовместимых с обеспечением международной стабильности и безопасности, что отрицательно отражается на целостности государств, поскольку наносит ущерб их собственной безопасности в военной и гражданской сферах.

2. Боливия обращает внимание на необходимость воспрепятствования использованию ресурсов, обеспечиваемых информационными технологиями, в преступных или террористических целях.

3. В этом контексте она предлагает для рассмотрения основные критерии, касающиеся информационной безопасности и несанкционированного вмешательства в имеющие к ней отношение системы.

Важность информации

4. Когда речь идет об информации, мы прямо или косвенно говорим о системах информатизации и телекоммуникаций (новых технологиях, новых формах использования — программное обеспечение, новых устройствах — жесткие диски, новых формах производства все более насыщенной, надежной и оперативной информации), оценивая прежде всего связанные с их использованием риски и степень их безопасности.

5. Необходимо иметь в виду, что место, куда стекается вся информация, может быть зачастую наиболее ценным и вместе с тем самым уязвимым объектом.

6. Проблема уязвимости телекоммуникаций касается также Интернета и телефонии. Интернет непосредственно связан с системами информатизации. Телефония подразделяется на сотовую и обычную, кабельную. Сотовая связь непосредственно примыкает к обычной среде распространения (пространству, в котором распространяются радиоволны), в которой пользователи оказываются погруженными в телефонный трафик и существует опасность перехвата их телефонных разговоров.

Хроника преступлений или преступных деяний в информационных системах

7. Побочные и случайные преступления, совершаемые с помощью компьютеров и приемных устройств, становятся все более частыми и разнообразными. В настоящее время большой процент совершаемых преступлений раскрывается случайно (обман, фальсификация, продажа информации).

8. Говоря об информационных системах, следует сказать об информационном вирусе как о программе, разработанной случайно или намеренно, на которую необходимо обратить особое внимание, и принять меры для противодейст-

вия этому явлению, установив с этой целью жесткие правила использования этих систем.

9. В вопросе о совершаемых преступлениях важно иметь в виду, что при возникновении каких-либо проблем необходимо выявить их причину и безотлагательно подумать о ее устранении. Среди наиболее опасных причин можно отметить следующие: личную выгоду, синдром «Робин Гуда», ненависть к организации, психические расстройства, непорядочность; в числе наименее опасных причин можно указать на выгоды для организации и игры.

Организационные парадигмы безопасности

10. В современной научной философии парадигмы играют важную роль и на них основаны правила, которыми руководствуются при проведении расследований.

11. В числе основных парадигм можно указать, в числе многих других, на следующие: ответственность за проведение аудита той или иной системы лежит на пользователе и ведомстве, отвечающем за внутренний аудит; системы безопасности не учитывают возможность мошенничества внутри системы; несчастные случаи в том или ином учреждении маловероятны; недостатки имеются везде, поскольку никакая система не является совершенной.

Оценка рисков

12. Очень важно, чтобы пользователи, работающие в том или ином ведомстве, осознавали, что информация всегда подвержена рискам, и понимали, что обеспечение безопасности является одной из их обязанностей. Для этого необходимо определить стоимость и качество системы безопасности, оценить ее с точки зрения рисков, выявить сферы применения, связанные с большой степенью риска, оценить количественный ущерб в случае прекращения предоставления услуг и разработать необходимые меры безопасности.

13. После определения степени риска необходимо составить перечень превентивных мер, которые должны быть приняты, а также мер по устранению последствий возможных катастроф, и установить их очередность.

14. Оценка и количественное определение рисков должны производиться на институциональном, государственном и региональном уровнях с указанием резервных программ, возможностей для их использования и для ликвидации последствий.

Задачи целостной системы безопасности

15. Разработать систему безопасности — значит планировать, организовывать, координировать, направлять и контролировать деятельность по сохранению и обеспечению гарантий целостности ресурсов, используемых для информационных целей, а также обеспечить защиту имущества учреждения, государства и региона.

16. С этой целью необходимо определить административные компоненты, политику в сфере обеспечения безопасности, определить и распределить обязанности, разработать меры на случай возникновения чрезвычайных ситуаций, определить цели в сфере безопасности, проанализировать ситуацию с точки зрения рисков и обеспечения информационной безопасности и в конечном счете разработать программу обеспечения безопасности.

Куба

[Подлинный текст на испанском языке]
[28 мая 2003 года]

1. Куба неизменно поддерживала резолюции, касающиеся «Достижений в сфере информации и телекоммуникаций в контексте международной безопасности», начиная с момента начала рассмотрения в 1998 году этого вопроса в Первом комитете Генеральной Ассамблеи Организации Объединенных Наций.

2. Включение этого вопроса в повестку дня Генеральной Ассамблеи свидетельствует о том, что международное сообщество осознало потенциальную опасность использования информационных технологий в немирных целях для международного мира и безопасности.

3. В ходе подготовки к проведению Всемирной встречи на высшем уровне по вопросам информационного общества и на самих этих встречах, одна из которых состоялась в Женеве в 2003 году, а другая состоится в Тунисе в 2005 году, вопрос, который является предметом вышеупомянутой резолюции и других непосредственно связанных с нею резолюций, был и остается в центре внимания международного сообщества.

4. Использование телекоммуникаций во враждебных целях с явным или тайным намерением подорвать правовую и политическую структуру государств является одной из форм противоправного использования этих средств, что может породить напряженность и ситуации, не благоприятные для международного мира и безопасности вразрез с принципами и целями Устава Организации Объединенных Наций.

5. В резолюции 57/53 прямо отмечается, что распространение и использование информационных технологий и средств затрагивает интересы всего международного сообщества и что широкое международное взаимодействие будет способствовать достижению оптимальной эффективности.

6. В восьмом пункте преамбулы резолюции выражается «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 целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам».

7. В пункте 3(b) постановляющей части к государствам-членам обращена просьба информировать о своей точке зрения и об оценках по вопросу определения основных понятий, относящихся к информационной безопасности, «включая несанкционированное вмешательство или противоправное использование информационных и телекоммуникационных систем и информационных ресурсов».

8. Под «несанкционированным вмешательством» Куба понимает использование этих систем без соблюдения международно принятых процедур и норм, в частности в рамках Международного союза электросвязи, и в нарушение соответствующих национальных положений.

9. Государства, которые еще не сделали этого, должны принять все необходимые меры для того, чтобы усилить национальные нормы и положения.

10. Кроме того, представляется необходимым проводить периодический обзор международных положений по этому вопросу, учитывая быстрые темпы развития соответствующих технологий, для того чтобы вносить изменения в эти нормы с учетом эволюции указанных технологий и тем самым сохранять эффективность и действенность этих международных положений.

11. Информационные и телекоммуникационные системы могут превратиться в оружие, если они разрабатываются и/или используются для причинения ущерба инфраструктуре того или иного государства. Это могут быть, например, внедрение в национальные сети с использованием иностранного программного обеспечения или с использованием внутренних источников самого государства, которые, однако, были созданы по инициативе другого государства или разработаны им; радио- и телепередачи, направленные на подрыв общественного порядка и конституционного строя другого государства, в которое поступают эти сигналы; действия, направленные на то, чтобы создать помехи и причинить ущерб службам радиовещания других государств или парализовать их работу, и так далее.

12. Куба вновь заявляет, что все государства обязаны уважать уже существующие международные нормы в этой сфере. Доступ к информационным или телекоммуникационным системам другого государства должен соответствовать заключенным международным соглашениям о сотрудничестве, при этом краеугольным камнем для решения этого вопроса должен быть принцип согласия затрагиваемого государства. Формы и масштабы обмена должны определяться на основе уважения законодательства того государства, к системе которого открывается доступ.

13. Международному миру и безопасности может быть причинен ущерб в результате агрессии того или иного государства против информационных или телекоммуникационных систем других государств. К сожалению, эти методы уже используются в качестве инструмента враждебной политики.

14. Куба является объектом такой агрессии, осуществляемой при содействии и с согласия правительства Соединенных Штатов, на протяжении почти 20 лет. Начиная с 1985 и 1990 годов, когда по распоряжению американского правительства начали свою незаконную деятельность соответственно радио- и телевизионная станции, нормальная работа кубинского радио и телевидения была нарушена в результате такого внедрения и созданных помех. Эти правительственные и прочие станции еженедельно транслируют на нашу страну программы объемом более 2220 часов, которые направлены на подрыв нашего конституционного порядка. Только для этих целей выделено 24 частоты.

15. Начиная с 1990 года правительство Соединенных Штатов выделяет на цели этой радио- и телевизионной агрессии более 20 млн. долл. США ежегодно.

16. Как отмечено в заявлении Министерства иностранных дел Республики Куба от 22 мая 2003 года, правительство Соединенных Штатов предприняло новые действия, означающие эскалацию радиоэлектронной и телевизионной агрессии, которая осуществляется против Кубы на протяжении десятилетий.

17. Радиостанция, которая была создана и используется правительством Соединенных Штатов для ведения подрывной работы против Кубы, с 20 мая 2003 года начала работать еще на четырех новых частотах, что создает помехи и снижает качество передач кубинского радио.

18. Эти действия являются открытым и грубым нарушением международного права, а также норм и положений, принятых Международным союзом электросвязи (МСЭ) — международной организацией, которая была создана для того, чтобы содействовать нормальному функционированию системы телекоммуникаций во всем мире, в частности положений его Регламента радиосвязи.

19. Во второй половине того же дня, 20 мая, официальные службы американской пропаганды передавали на Кубу с борта самолета EC-130 военно-воздушных сил США с теми же целями с 18 ч. 00 м. до 22 ч. 00 м. телевизионный сигнал на каналах, официально выделенных кубинским телевизионным станциям и должным образом зарегистрированных в указанной международной организации.

20. Эти действия также являются нарушением международного права и норм, согласованных всеми государствами в рамках Международного союза электросвязи, в частности правила 23.3 его Регламента радиосвязи, в котором запрещается вести телевизионные передачи за пределами национальных границ.

21. Эти телевизионные передачи осуществляются также в нарушение положений преамбулы Устава Международного союза электросвязи, поскольку речь идет о деятельности, которая не содействует обеспечению мирных связей, международному сотрудничеству и экономическому и социальному развитию народов с помощью эффективно действующей электросвязи.

22. Поэтому Куба не приемлет и осуждает терпимость американских властей в отношении деятельности террориста Хосе Басульто и его намерений передавать телевизионные сигналы на кубинскую территорию. Несмотря на то, что по дипломатическим каналам была своевременно передана информация о том, что г-н Басульто предупрежден, что любая передача на Кубу будет рассматриваться как нарушение американского закона и поэтому против него будут приняты соответствующие меры, этот известный террорист беспрепятственно совершил 20 мая полет, и если передача все-таки не состоялась, то только потому, что у него возникли проблемы с передатчиком, который он намеревался использовать, а вовсе не из-за противодействия американских властей, которые вели себя как откровенные соучастники.

23. Согласно правилу 15.34 Регламента радиосвязи МСЭ, телевизионная агрессия Соединенных Штатов создает вредные помехи, исходящие от телевизионной станции, которая работает на канале 13 ОВЧ (210–216 МГц), что серьезно нарушило работу кубинских телевизионных служб, должным образом зарегистрированных на указанном канале.

24. Ведающие вопросами радиосвязи кубинские власти информировали об этом факте Федеральную комиссию по связи (ФКС) правительства Соединенных Штатов, ясно указав все технические и юридические параметры, которые были грубо нарушены.

25. Куба готовит также протест в связи с имевшими место описанными фактами на имя Генерального секретаря Международного союза электросвязи и намерена обратиться к нему с просьбой принять по этим фактам соответствующие меры.

26. Куба считает необходимым укрепить международные юридические основы в сфере информации и телекоммуникаций. Она считает также совершенно

необходимым уважать уже установленный в этой сфере международный порядок на основе безусловного осуществления положений международного права и Устава Организации Объединенных Наций, которые должны превалировать в отношениях между государствами. В этой сфере уже существуют аналогичные международные принципы, положения и процедуры, которые необходимо соблюдать.

27. Необходимо приложить усилия для разработки не являющихся юридически обязательными принципов и принятия соответствующих норм в рамках международных многосторонних и юридически обязательных протоколов или конвенций.

28. При использовании обеих этих методологий необходимо учитывать такие основные критерии, как несанкционированное вмешательство или противоправное использование информационных и телекоммуникационных систем и информационных ресурсов; связанные с этими темами аспекты суверенитета; использование средств информации и телекоммуникаций во всех их аспектах в мирных целях; содействие международному сотрудничеству для оказания помощи в развитии информационных и телекоммуникационных систем в развивающихся странах, учитывая решающее воздействие информационных технологий и коммуникаций на процесс социально-экономического развития; предотвращение, противодействие и искоренение враждебной практики использования этих систем и применение национальных мер, которые позволили бы государствам установить более эффективный контроль над информационными и телекоммуникационными системами и противодействовать соответствующим преступным действиям.

29. В дополнение к уже изложенным элементам Куба считает необходимым обратить внимание на следующие аспекты, которые имеют непосредственное отношение к использованию в полном объеме телекоммуникаций в качестве инструмента укрепления международного мира и безопасности:

– все государства обязаны воздерживаться от применения односторонних мер принудительного характера, противоречащих международному праву, которые ограничивают доступ затрагиваемого государства к технологиям и международным сетям обмена информацией и коммуникаций;

– системы сертификации и возможные санкции в отношении какого-либо государства в вопросах доступа к телекоммуникационным технологиям или иным, тесно связанным с ними технологиям с точки зрения угрозы международному миру и безопасности, должны быть многосторонними по своему характеру и разрабатываться на основе моделей, согласованных международным сообществом;

– необходимо использовать потенциал международного сотрудничества в данной сфере, задействовав все необходимые ресурсы для оказания помощи развивающимся странам в укреплении и расширении их телекоммуникационных систем;

– необходимо принять законодательные и иные меры как на национальном, так и на международном уровнях, чтобы не допустить неоправданной концентрации в руках частных лиц собственности и средств контроля над средствами телекоммуникаций, а также других средств информации и телекоммуникации, учитывая, что они препятствуют необходимой диверси-

фикации источников информации, а также то обстоятельство, что они могут быть использованы в качестве инструмента для подрыва мира и подстрекательства к войне;

– необходимо установить многостороннюю, межправительственную, демократическую и транспарентную систему управления и контроля за Интернетом и другими международными сетями информации и коммуникаций. Жизненно важное значение имеет требование о наличии межправительственной системы контроля;

– системы контроля и наблюдения за средствами телекоммуникаций и другими формами международных коммуникаций должны быть многосторонними и транспарентными по своему характеру и предусматривать четко установленную ответственность и процедуры их проверки общественностью для того, чтобы положить конец вмешательству в частную жизнь, а также нарушениям суверенитета и безопасности многих государств со стороны глобальных систем шпионажа, созданных некоторыми индустриальными державами, в частности Соединенными Штатами;

– обеспечение прочных гарантий уважения культурного разнообразия, которые позволили бы покончить с любой формой дискриминации или пропаганды ненависти в информационных материалах, распространяемых в рамках телекоммуникационных систем на международном уровне.

Сальвадор

[Подлинный текст на испанском языке]
[30 июня 2003 года]

Ответ правительства Сальвадора на просьбу, содержащуюся в пункте 3 постановляющей части резолюции 57/53 Генеральной Ассамблеи, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»

1. Статья 24 Конституции Республики запрещает создавать помехи и внедряться в телефонную связь — таковы конституционные положения, которые действуют в настоящее время в Сальвадоре в сфере информационной и телекоммуникационной безопасности.

2. Статьи 184, 185, 186 и 302 Уголовного кодекса предусматривают наказание за незаконное завладение письменным сообщением, вспомогательным документом или любым другим документом или личным документом, который не предназначен лицу им завладевшему, или за предоставление конфиденциальных личных данных о каком-либо лице или семье; за действия, связанные с перехватом сообщений, такие, как перехват или нарушение телеграфной или телефонной связи, с использованием технических средств для прослушивания или записи указанных сообщений.

3. Такие случаи не являются преступлениями, когда речь идет об угрозах, об освобождении того или иного лица, которое было лишено свободы или похищено, или об организованных преступлениях и жертвах, пострадавший или их представитель, соответственно, обращаются в Генеральную прокуратуру Республики с письменной просьбой о прослушивании и записи разговоров или

действий, в ходе которых они получают такие угрозы или требования или дают письменное согласие на их прослушивание и запись.

4. Применение регулирующих положений в сфере телекоммуникаций и применение административных санкций является компетенцией Главного управления энергетики и телекоммуникаций согласно положениям статьи 4 закона о его создании и статьи 29(b) закона о телекоммуникациях, в которых гарантируется охрана тайны сообщений.

5. В 2001 и 2002 годах в Законодательное собрание был направлен проект закона о внесении соответствующих изменений в Конституцию Республики, которые позволяли бы внедряться и/или прослушивать телефонные разговоры в качестве средства борьбы с организованной преступностью и торговлей наркотиками. На сегодняшний день этот проект пока не одобрен.

Грузия

[Подлинный текст на английском языке]
[24 июня 2003 года]

1. Правительство Грузии занимается в настоящее время разработкой национальной стратегии в области информации, направленной на развитие средств телекоммуникаций и создание новых технологий, понимая при этом важность осуществления государственной политики для обеспечения гарантий использования информационных технологий.

2. Кроме того, правительство Грузии проводит политику, направленную на интегрирование Грузии в глобальное информационное общество, опять же осознавая при этом все риски и трудности, которые сопряжены с обеспечением безопасности информации.

3. Правительство Грузии считает исключительно важным участие в международных программах и совместных проектах, направленных на установление более защищенного международного информационного общества, понимая при этом, что существующее реальное положение дел в сфере информационных технологий и систем, а также особенности региона, в котором находится Грузия, не позволяют решать вопросы информационной безопасности в одностороннем порядке.

Российская Федерация

[Подлинный текст на русском языке]
[28 апреля 2003 года]

Вопросы, связанные с работой группы правительственных экспертов по проблеме информационной безопасности

1. В соответствии с принятыми консенсусом резолюциями Генеральной Ассамблеи Организации Объединенных Наций «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» №№ 56/19 от 29 ноября 2001 года и 57/53 от 22 ноября 2002 года в 2004 году создается группа правительственных экспертов. В данных резолюциях содержится поручение группе правительственных экспертов рассмотреть существующие и потенциальные угрозы в сфере информационной безопасности, возможные совместные меры по их устранению, провести исследование международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем, и представить доклад о результатах данного исследования Генеральной Ассамблее Организации Объединенных Наций на ее шестидесятой сессии.

2. Российская Федерация отмечает сохраняющуюся важность и возрастающую актуальность темы международной информационной безопасности и полагает, что в настоящее время информационная безопасность является важным аспектом национальной безопасности государств, а также частью общей системы международной безопасности и стратегической стабильности. Вопросы использования информационно-телекоммуникационных технологий и средств имеют непосредственное отношение к обеспечению военно-политической безопасности стран во всем мире и, следовательно, требуют глобального, всеобъемлющего и недискриминационного подхода на основе участия в рассмотрении данного вопроса возможно большего числа стран и принципа равного географического представительства.

3. Именно такой подход способна обеспечить работа под эгидой Организации Объединенных Наций, чей потенциал как центральной международной организации, наиболее полно представляющей интересы всех стран и играющей координирующую роль в области разоружения, позволяет формировать на ее основе сбалансированную и эффективную систему глобальной безопасности.

4. Считаем, что в плане исследования всего комплекса вопросов, связанных с проблематикой международной информационной безопасности, а также выработки соответствующих рекомендаций полезную роль сыграли резолюции Генеральной Ассамблеи Организации Объединенных Наций №№ 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года и 57/53 от 22 ноября 2002 года, традиционно принимающиеся консенсусом и, следовательно, отражающие взгляды на данную проблему всего мирового сообщества, а также соответствующие вклады государств по проблеме информационной безопасности, содержащиеся в докладах Генерального секретаря Организации Объединенных Наций A/54/213, A/55/140 и Corr.l и Add.l, A/56/164 и Add.l и A/57/166 и Add.l.

5. В плане выявления подходов, имеющихся в настоящее время в отношении вопросов международной информационной безопасности, важную роль сыграл

организованный в соответствии с рекомендациями резолюции 53/70 Институтом Организации Объединенных Наций по проблемам разоружения и Департаментом по вопросам разоружения Секретариата Организации Объединенных Наций в августе 1999 года в Женеве международный семинар по вопросам международной информационной безопасности, в котором приняли участие представители более 50 стран.

6. Семинар подтвердил актуальность проблемы информационной безопасности и своевременность постановки этого вопроса в международном плане, а также позволил обозначить различные подходы к рассмотрению существа проблемы. В настоящее время не существует общепринятых и адекватных международных норм или инструментов, в которых рассматривались бы вопросы информационной безопасности с точки зрения мер по уменьшению существующих и потенциальных опасностей в этой сфере в глобальном масштабе.

7. В этой связи представляется необходимым совместно, при возможно полном представительстве стран, изучить существующие на этот счет концепции и подходы, а также провести анализ имеющихся на данный момент международно-правовых документов по различным аспектам международной информационной безопасности.

8. Полагаем, что международное многостороннее обсуждение данной проблематики вступает в качественно новую фазу, связанную с созданием группы правительственных экспертов по проблеме информационной безопасности. Группа правительственных экспертов предоставляет мировому сообществу уникальную возможность для изучения всего комплекса упомянутых выше вопросов.

9. Российская Федерация хотела бы принять конструктивное участие в работе группы правительственных экспертов и хотела бы, в этой связи, высказать некоторые соображения относительно вопросов, которые, по нашему мнению, могли бы составить повестку дня ее работы.

10. Рассматривая проблемы международной информационной безопасности, требуется, прежде всего, исходить из таких общечеловеческих ценностей, как гарантированность универсального, свободного, равноправного и безопасного международного информационного обмена на основе общепризнанных норм и принципов международного права.

11. В ходе работы данной группы необходимо было бы учитывать вклады государств, полученные в соответствии с известными резолюциями Генеральной Ассамблеи Организации Объединенных Наций по международной информационной безопасности, и другие материалы, которые могут быть представлены на рассмотрение членами группы.

12. Как нам видится, группа могла бы сконцентрировать обсуждение на следующих ключевых, с нашей точки зрения, моментах.

13. Во-первых, согласовать соответствующий понятийный аппарат в сфере международной информационной безопасности. Важными задачами данного этапа деятельности группы правительственных экспертов могли бы стать выработка основных базовых определений: информационных сетей, ресурсов и систем, информационных инфраструктур, информационного оружия, а также

выявление характера, признаков, типологии и классификация угроз информационной безопасности.

14. Во-вторых, рассмотреть факторы, влияющие на состояние международной информационной безопасности. Информационная безопасность представляет собой сложную и комплексную сферу, требующую к себе со стороны международного сообщества всеобъемлющего подхода с учетом наличия угроз как террористического или криминального, так и военного характера, как в военной, так и в гражданской областях.

15. В складывающемся глобальном информационном обществе информационно-коммуникационные технологии взаимосвязаны и обладают свойством трансграничности. Как следствие, в рамках глобального информационного общества международная информационная безопасность оказывается неразрывно и естественно сопряженной с вопросами идентификации источника угроз в отношении их внутреннего или внешнего характера, вопросами национального суверенитета государств, задачей уважения прав и свобод человека, в частности права на невмешательство в частную жизнь. Эти и связанные с ними вопросы могли бы дать почву для обсуждений в ходе работы группы правительственных экспертов.

16. Следующим этапом могло бы стать определение взаимоприемлемых мер предотвращения использования информационных технологий и средств в террористических и других преступных целях, а также мер по ограничению применения информационного оружия, прежде всего в отношении критически важных структур государств. Задачами данного этапа, как видится, стало бы рассмотрение возможности разработки процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия, создания системы международного мониторинга для отслеживания угроз, проявляющихся в информационной сфере, и механизма контроля выполнения условий режима международной информационной безопасности, равно как и механизма 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.

17. Следовало бы подумать о возможных путях международного взаимодействия правоохранительных органов по предотвращению и пресечению правонарушений в информационном пространстве, в частности, по выявлению источников информационной агрессии; взглянуть на проблему сопряжения национальных законодательств отдельных стран в части, регулирующей вопросы информационной безопасности с тем, чтобы обеспечить унифицированную классификацию правонарушений в сфере информационной безопасности и ответственность, возникающую в связи с совершением действий, классифицируемых как преступные.

18. Предложили бы также оценить возможности оказания международной помощи странам, ставшим жертвами информационных атак в целях смягчения последствий нарушения нормальной деятельности прежде всего объектов критических инфраструктур государств.

19. В перспективе, возможно, следует стремиться к выработке многостороннего, взаимоприемлемого международно-правового документа, направленного

на укрепление режима международно-правовой безопасности, в соответствии с которым государства и другие субъекты международного права должны будут нести международную ответственность за деятельность в информационном пространстве, осуществляемую ими или с территорий, находящихся под их юрисдикцией.

20. Основной идеей создания универсального режима международной информационной безопасности, по мнению Российской Федерации, могло бы стать обязательство участников не прибегать к действиям в информационном пространстве, целью которых является нанесение ущерба информационным сетям, системам, ресурсам и процессам другого государства, его инфраструктуре, подрыв политической, экономической и социальной систем, массированная психологическая обработка населения, с целью дестабилизации общества и государства.

Сенегал

[Подлинный текст на французском языке]
[9 июня 2003 года]

1. Меры, связанные с безопасностью в сфере дистанционной обработки и передачи данных, имеют важное значение для обмена информацией, в частности касающейся оборота оружия. Необходимо обеспечивать конфиденциальность такой информации.

2. Следовательно, нужно защищать такую информацию, для чего необходимо решить определенные задачи, а именно:

3.– достижение безопасности аппаратных средств, программного обеспечения и систем обработки данных на основе внедрения усовершенствованных технических устройств;

4.– обеспечение безопасности процедур обмена информацией на основе применения четких и единообразных протоколов.

Украина

[Подлинный текст на русском языке]
[27 мая 2003 года]

1. Общая оценка проблем информационной безопасности

1. Международные процессы глобализации, внедрения новейших информационных технологий, формирование информационного общества усиливают значимость такой составляющей национальной безопасности, как информационная безопасность.

2. Развитие информационной инфраструктуры государства, создание и внедрение новых информационных технологий вызывают появление определенных угроз информационной безопасности. Наиболее важными среди них являются намеренные угрозы, источником которых могут быть объективные и субъективные отличия духовных, интеллектуальных и материальных интересов

субъектов информационных взаимоотношений, а также путей, форм и методов их удовлетворения, что, в целом, может стать причиной конфликтной ситуации.

3. К основным угрозам информационной безопасности относятся:

– манипулирование информацией (дезинформация, утаивание или перекручивание информации);

– нарушение установленного порядка информационного обмена, несанкционированный доступ или необоснованное ограничение доступа к информационным ресурсам, противоправный сбор и использование информации;

– разрушение информационного пространства государства или его использование в антигосударственных интересах;

– информационный терроризм, например распространение компьютерных «вирусов», установка программных и аппаратных закладных устройств, внедрение радиоэлектронных устройств перехвата информации в технических средствах и жилищах, незаконное использование информационных и телекоммуникационных систем и информационных ресурсов, навязывание фальшивой информации и т .д.

4. Непосредственным результатом негативных информационных влияний является искажение информации, что приводит к деформации и/или разрушению информационной среды государства и ее информационных ресурсов, невозможности функционирования важных государственных, производственных, финансовых, научных и общекультурных систем и, как следствие, к утрате национального информационного суверенитета.

5. Таким образом, анализ проблем информационной безопасности показывает, что к наиболее общим относятся проблемы поддержания необходимого объема и качества информационных ресурсов, разработки стратегии их использования и соответствующих информационных технологий, создания адекватной информационной инфраструктуры, поддержания безопасности информации в информационных и телекоммуникационных системах, а также борьбы с негативными информационными влияниями на личность, общество и государство в целом.

6. Недостаточный уровень защищенности информационных ресурсов государства может привести к значительному экономическому ущербу за счет обесценивания и потери их товарной части — промышленных и информационных технологий, а также к нанесению значительного ущерба национальной безопасности в целом вследствие возможных нарушений нормального функционирования систем связи, контроля и управления, утечки информации, составляющей государственную тайну, и т.п.

7. Информационная безопасность предполагает проведение мероприятий по защите информации на всех этапах работы с нею. Целью информационной безопасности является обеспечение целостности системы, защита и гарантия точности и целостности информации, а также минимизация последствий, которые могут возникнуть в том случае, если информация будет модифицирована или уничтожена.

8. Объективной реальностью современного мира является использование в разных сферах жизнедеятельности общества и государства локальных и глобальных информационных систем, предназначенных для ускорения обмена информацией и доступа к разнообразным информационным ресурсам.

9. Широкое внедрение таких систем, в частности в те сферы деятельности, которые связаны с управлением государством, создает реальные возможности для несанкционированного доступа к информационным ресурсам государства и систем управления ими, распространения сообщений противоправного содержания, нарушения целостности и доступности информации и т.д.

10. Стабильность функционирования политической, экономической, военной, кредитно-финансовой и других сфер государства зависит не только от эффективности, но и от надежности функционирования телекоммуникационных и информационных систем. В условиях создания информационного пространства особую остроту и актуальность приобретают вопросы надежности и защищенности информационно-телекоммуникационных систем, функционирующих в интересах управления государством. Имея доступ к информационным системам, можно не только получать важную информацию, но и путем нарушения или блокирования работы информационных систем полностью или частично парализовать деятельность жизненно важных объектов и даже целых областей хозяйства, оказывать негативное влияние на информационные ресурсы, распространять запрещенную законодательством информацию и т.п.

11. Обеспечение безопасности информации, циркулирующей в ИТС, является одним из главных факторов и необходимым условием обеспечения информационной безопасности, национального и государственного суверенитета, устойчивости общественного развития.

12. На данном этапе развития информационно-телекомуникационных систем основными среди угроз для информации, которая в них циркулирует, являются:

– нарушение штатного режима функционирования важных информационных и телекоммуникационных систем;

– случайные или намеренные действия, вызвавшие нарушение конфиденциальности, целостности и доступности информации;

– разжигание информационного противостояния (распространение компьютерных «вирусов», установка программных и аппаратных закладных устройств, внедрение радиоэлектронных устройств перехвата информации в технических средствах и помещениях, перехват и дешифрирование информации, навязывание фальшивой информации, радиоэлектронное влияние на парольно-ключевые системы, радиоэлектронное подавление линий связи и систем управления и т .д.).

13. Надежную защиту информационно-телекоммуникационных систем, прежде всего органов государственного управления, от преступных посягательств можно обеспечить только путем внедрения комплексной системы защиты информации, которая включает использование криптографических и технических средств защиты, а также выполнение ряда организационных и технических мероприятий.

14. Особого внимания требует проблема подсоединения компьютерных сетей к международным информационным сетям.

15. Полноценное вступление Украины в международное сообщество невозможно без расширения информационного взаимодействия с глобальными информационными сетями передачи данных, такими, как Интернет. Такие системы предоставляют большой набор современных информационно-телекоммуникационных услуг, многие из которых рекламируются как такие, которые обеспечивают информационную защиту.

16. В то же время большое количество средств, использующихся в таких системах, специальные свойства которых при отсутствии исходящих текстов программ оценить очень тяжело, а то и невозможно, представляют угрозу безопасности информации, финансовых трансакций и электронных платежей. Известны многочисленные примеры непродуманного использования банками импортных информационных технологий, позволяющих специалисту проникнуть в систему за время одного десятиминутного сеанса связи.

17. Необходимо обратить внимание на опасность непродуманного подключения к глобальным сетям абонентских пунктов и локальных сетей. Практически любая локальная компьютерная сеть, подключенная к Интернету без использования соответствующих мероприятий защиты, становится легкодоступной для «хакеров».

18. Переход к новым формам и способам реализации информационных общественных отношений, в частности широкое распространение новых видов предпринимательской деятельности с использованием сети Интернет (электронной коммерции), а также постепенное внедрение системы электронного правительства, сопровождается широким использованием компьютерных технологий и увеличением объемов информации в электронном виде. Это обусловливает увеличивающуюся зависимость субъектов информационных отношений от степени защищенности такой информации, которая, в свою очередь, становится объектом внимания негативно настроенных субъектов общества и их группировок. Несоответствие существующих систем и механизмов защиты обусловливает появление реальных условий для несанкционированного доступа, использования, блокирования или разрушения информации, которая создается, обрабатывается, передается и хранится в электронном виде.

19. В целом, проблема вмешательства в информационные ресурсы государства является актуальной для всего мира. Если до начала 90-х годов наиболее острыми были вопросы защиты государства от иностранных разведок, то в последнее время в связи с широким внедрением во все сферы общественной жизни информационных технологий на первый план вышла проблема противодействия так называемым компьютерным преступлениям. Об этом может свидетельствовать тот факт, что компьютерные преступления признаны на международном уровне как новый вид интеллектуальных преступлений. При этом преступления в этой сфере совершаются не только организованными преступными группировками, но и террористическими организациями и отдельными нарушителями.

20. Наиболее привлекательными для преступников являются информационные системы органов государственной власти, правоохранительных, таможенных, налоговых органов, учреждений кредитно-финансовой, военной сферы и т.д. В частности, в Украине правоохранительными органами неоднократно фиксировались противоправные операции, связанные с использованием пластиковых карточек международных платежных систем, а также формированием

фиктивных электронных платежей с целью незаконного получения денег, вмешательства в работу компьютерных сетей через Интернет и т .д.

2. Определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или противоправное использование информационных и телекоммуникационных систем и информационных ресурсов

21. В условиях стремительного развития информационных и телекоммуникационных технологий острой становится проблема обеспечения информационной безопасности, в том числе решение проблем несанкционированного вмешательства или противоправного использования информационных и телекоммуникационных систем, а также защита информационных ресурсов.

22. При этом под термином «информационная безопасность» необходимо понимать такое состояние защищенности информационного пространства государства, при котором реализуются национальные интересы и соблюдаются права личности, общества и государства.

23. Учитывая высокую общественную опасность указанных неправомерных действий и принимая во внимание важность эффективного функционирования информационно-телекоммуникационных систем, в Криминальном кодексе Украины определены преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и предусмотрены соответствующие наказания за содеяние таких преступлений, в частности:

– незаконное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей — действия, которые привели к перекручиванию или уничтожению компьютерной информации или носителей такой информации, а также распространение компьютерных вирусов путем применения программных и технических средств, предназначенных для незаконного проникновения в такие машины, системы или компьютерные сети;

– похищение, присвоение, вымогательство компьютерной информации или завладение последней путем обмана или злоупотребления служебным положением;

– нарушение правил эксплуатации автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей лицом, ответственным за их эксплуатацию, — действия, которые стали причиной похищения, перекручивания или уничтожения компьютерной информации, средств ее защиты, незаконное копирование компьютерной информации или существенное нарушение работы таких машин, их систем или компьютерных сетей.

24. Обобщая, термин «компьютерное правонарушение» можно определить как противоправное действие, которое посягает на установленный порядок функционирования информационных систем и режима доступа к ним, нарушает целостность, конфиденциальность или доступность информации, права и свободы граждан во время информационной деятельности.

3. Содержание международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем

25. Двадцать первое столетие должно войти в историю как период становления и развития глобального информационного общества, которое заменит или дополнит материальные процессы информационными, а также будет способствовать существенному повышению продуктивности труда и повышению общественного благосостояния. Многие страны уже создают организационно-техническую основу для национальной и глобальной инфраструктуры. ООН рассматривает вопрос о внесении права на доступ к базовым средствам связи и информации в Декларацию основных прав человека.

26. Опыт развитых стран по эффективному решению проблемы информатизации, во второй половине 90-х годов, обобщенный международными (ITU, ISO/IEC, ETSI) и многочисленными национальными организациями по стандартизации, убеждает в необходимости создания многоуровневых (национальных и региональных) информационных инфраструктур с последующим объединением в Глобальную информационную инфраструктуру GII (Global Information Infrastructure).

27. Причастность Европы к GII означает не только создание в рамках региона EII, но и содействие построению национальных информационных инфраструктур в отдельных странах для достижения взаимной выгоды каждой страны и Европы в целом. Вместо использования термина EII европейцы отдают преимущество использованию термина «Европейское информационное сообщество» — EIS (European Information Society). Конструктивными блоками EIS являются сети, базовые услуги и дополнения. Существующие в Европе сети могут быть усилены реализацией европейской широкополосной супермагистрали, которая объединяет в единое целое европейские телекоммуникационные, кабельные и спутниковые сети. Страны Европы поддерживают использование трансъевропейских базовых услуг, включая услуги электронной почты, передачу файлов и видео.

28. Европейские страны также уделяют большое внимание социальному аспекту очередного этапа мировой технологической революции. Резолюции и документы Совета Европы посвящены формированию национальной политики в сфере построения информационного общества. При этом вышеуказанное задание воспринимается не как дань моде, а как необходимое условие развития, неприятие которого ведет к потере темпов и отходу от передовых экономических и технологических позиций.

29. Мировые тенденции правового регулирования деятельности в сфере новейших технологий передачи данных свидетельствуют о необходимости разработки единых подходов к созданию законодательных и нормативных актов для всех участников международного информационного обмена. Согласно выводу Американской коллегии юристов, на сегодня существует реальная потребность в создании многонациональной комиссии по законотворчеству в киберпространстве. Среди перечня решений, рекомендуемых для рассмотрения будущей комиссией, одним из важнейших является создание кибертрибунала. В современных условиях главной проблемой правового обеспечения информационной безопасности является необходимость приведения существующих правовых норм в соответствие с достижениями информационных технологий.

30. Сегодня невозможно представить информационное пространство без компьютерной сети. Именно эти технологии дали толчок возникновению и развитию многих видов бизнеса: электронным расчетным карточкам, оперативным межбанковским расчетам, обслуживанию бирж, брокерским конторам и т.д.

31. Ожидается, что к 2005 году половина населения ЕС будет иметь доступ в Интернет. Поэтому страны ЕС направляют свои усилия на закрепление доверия к коммерческим и финансовым операциям через Интернет, а также ускорение перехода к электронной коммерции.

32. Европейский парламент 7 мая 1999 года согласовал законопроект ENFOPOL 98, который дает право компетентным органам законным образом осуществлять мониторинг сетей. Законопроект представляет собой проект резолюции Совета ЕС «Относительно законного мониторинга телекоммуникаций с учетом новых технологий». Документ призывает сделать доступными для органов, которые будут осуществлять мониторинг в реальном времени, все телекоммуникационные сети, включая Интернет и спутниковые системы телефонной связи. В свою очередь, британское правительство начало реализацию проекта по созданию Центра, который будет заниматься перехватом всего электронного трафика внутри страны.

33. Правительство Китая для осуществления контроля над доступом в сеть идет путем лицензирования использования модемов, а все потоки информации Интернета направляются через ограниченное количество национальных операторов.

34. Среди проблем информационной безопасности можно выделить следующие:

– нарушение прав интеллектуальной собственности;

– распространение информации, негативно влияющей на социальное здоровье людей, в том числе проблемы, связанные с доступом детей в Интернет;

– проведение незаконных коммерческих операций;

– несанкционированный доступ к конфиденциальной информации;

– нарушение прав и законных интересов личности в процессе обмена информацией;

– распространение недоброкачественной рекламы.

35. Существует еще одна опасность Интернета, которая заключается в возможности использования конфиденциальной информации личности без ее решения. Собирать такие сведения можно, анализируя информацию, которой лицо пользуется в Интернете.

36. Интернет — очень специфическое средство коммуникации и вследствие своего трансграничного характера трудно поддается правовому регулированию. Все участники Интернета подпадают под действие законов своих стран. В то же время незаконное содержание может быть выявлено не на территории той страны, где оно хранится на сервере. В связи с этим для урегулирования правовых отношений в Интернете необходимы международные соглашения, принятие которых, в свою очередь, осложняется разными подходами законодательст-

ва государств к тем или иным правонарушениям, например разное значение вкладывается в понятие «порнография». На сегодня общее направление законодательных инициатив в сфере Интернета направлено на установление ответственности провайдеров хостовых услуг за содержание информации, содержащейся на их компьютерах. Поскольку это очень сложно с технической точки зрения, в законодательстве некоторых стран ответственность провайдеров обусловливается тем, что они знали о содержании незаконной информации.

37. Интерпол, который объединяет правоохранительные органы 178 стран мира, сообщил о том, что будет размещать информацию по сетевым преступлениям на сайте американской компании Atomic Tangerine. Интерпол предоставит сведения о хакерах, а также о видах преступлений, которые угрожают компаниям, занимающимся электронным бизнесом. Atomic Tangerine, в свою очередь, должна обеспечивать международную полицейскую организацию информацией, полученной при помощи «системы раннего предупреждения» NetRadar, которая принадлежит компании и предназначена для осуществления мониторинга в Сети.

38. Одной из важных проблем является проблема анонимности сообщений, которая осложняет, а иногда и делает невозможным установление личности владельца незаконной информации, а также привлечение его к ответственности. Поэтому эксперты многих стран предлагают законодательно закрепить запрещение анонимных сообщений, разрешив при этом сообщения под псевдонимом, по которым при необходимости можно было бы установить автора.

39. 21 декабря 1998 года Совет ЕС утвердил предложенный Европарламентом план действий по безопасному использованию Интернета. План действовал четыре года (с 1 января 1999 года по 31 декабря 2002 года). Его бюджет составлял 25 млн. евро. Согласно плану, предполагалось создание разных «уровней качества» Интернета, которые должны формироваться в соответствии со «знаками Интернет-качества» продукции. Эти положения должны были быть закреплены как в национальных законодательствах, так и в кодексах саморегулирования Интернет-провайдеров. В марте 1999 года Европейская комиссия по результатам обсуждения положений Доклада о конвергенции телекоммуникаций, СМИ и информационных технологий приняла отчет, основным выводом которого, в частности, было следующее положение: правовое регулирование в Интернете должно носить прозрачный, ясный и пропорциональный характер.