Организация Объединенных Наций A/64/129

Генеральная Ассамблея

Distr.: General
8 July 2009
Russian
Original: English/Russian/Spanish

Шестьдесят четвертая сессия
Пункт 90 первоначального перечня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Содержание

* A/64/50.

09-39635 (R) 300709 030809

I. Введение

1. В пункте 3 совей резолюции 63/37 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) усилия, предпринимаемые на национальном уровне для укрепления национальной безопасности и содействия международному сотрудничеству в этой области;

c) содержание концепций, упомянутых в пункте 2 указанной резолюции;

d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне.

2. В соответствии с этой просьбой 27 февраля 2009 года государствам-членам была направлена вербальная нота, в которой им предлагалось представить информацию по данному вопросу. Полученные ответы содержатся в разделе II ниже. Любые ответы, полученные дополнительно, будут изданы в качестве дополнений к настоящему докладу.

II. Ответы, полученные от правительств

Бразилия

[Подлинный текст на английском языке]
[11 июня 2009 года]

1. Информатизация и телекоммуникации являются важной составляющей жизни современного общества, которое в значительной степени полагается на них. Современная деятельность в значительной степени зависит от наличия постоянного доступа к подобным услугам, что делает их весьма ценным ресурсом, имеющим определяющее значение для благосостояния и процветания государств.

2. Технологические достижения, позволившие воплотить этот сценарий в жизнь, также создали ряд проблем в контексте международной безопасности. Поскольку общество все более зависит от доступности информации и телекоммуникационной инфраструктуры, повышается степень его уязвимости, и это может быть использовано во время военных конфликтов, а также в преступных и террористических целях.

3. Подобного рода действия могут стать потенциальной угрозой для деятельности частных компаний, банков, фондовых рынков и правительственных организаций. Растущая взаимосвязь между базовыми сетями коммуникаций, будучи, безусловно, полезной, провоцирует ряд новых проблем, которые государства должны решать на национальном и международном уровнях.

4. Достижения в сфере информатизации и телекоммуникаций могут не только повысить уязвимость общества, но и использоваться в качестве «кибероружия». В вооруженных силах ряда стран уже имеются специальные военные подразделения, получившие соответствующую подготовку и располагающие техническими средствами для осуществления подрывных действий или даже уничтожения критически важной инфраструктуры через вмешательство в информационные сети и нарушение их работы. В зависимости от целей и используемых средств подобные атаки могут привести как к «программируемому» уничтожению вражеских оружейных или наблюдательных систем, так и к глобальному срыву работы общенациональных энергетических систем.

5. Повышению эффективности подобного рода военных действий способствует и то, что для обеспечения многих таких возможностей необходимы относительно небольшие финансовые вложения. С учетом этих факторов война в киберпространстве в ближайшем будущем вполне может стать следующим этапом военных межгосударственных конфликтов. Такую же тактику могут использовать отдельные террористы или организации.

6. Осознавая важность данного вопроса для поддержания международного мира и безопасности, Бразилия предлагает решать этот вопрос с двух точек зрения. Во-первых, международному сообществу следует стремиться к созданию соответствующих механизмов борьбы с преступной и террористической деятельностью, основанной на использовании информационных технологий. В рамках отдельного или дополняющего подхода следует также учитывать последствия возникновения кибероружия и потенциальную необходимость создания режимов разоружения и нераспространения, которые бы учитывали многочисленные аспекты этого рода враждебных действий.

7. Необходимо должным образом обсуждать преступную и террористическую деятельность на соответствующих форумах, а Организация Объединенных Наций должна играть соответствующую роль в оказании требуемого содействия государствам-членам, в частности в реализации следующих целей:

- создание аварийных и резервных сетей для защиты критически важной инфраструктуры;
- анализ сетевой структуры с учетом взаимозависимых элементов, а также выявление эффективных методов защиты;
- тесное сотрудничество между правительством и частным сектором, направленное на обеспечение необходимого уровня безопасности при обмене информацией между организациями;
- создание защитных систем для устранения или минимизации последствий кибератак;
- применение механизмов и мер, позволяющих властям отслеживать источник кибератак;
- обсуждение целесообразности и полезности международных юридически обязывающих механизмов в отношении киберпреступлений;
- аттестация национальных институтов для осуществления проверки и оценки уровня безопасности информационных систем;

- определение процедур взаимного уведомления о киберугрозах между соответствующими национальными ведомствами;
- устранение дискриминационных механизмов, которые могут воспрепятствовать странам в получении доступа к высоким технологиям в сфере телекоммуникационных и информационных систем;
- просветительская работа и информирование общественности о значении кибербезопасности.

8. Организация Объединенных Наций также должна играть ведущую роль в дискуссиях об использовании информатизации и телекоммуникаций как средств ведения кибервойны в ситуациях межгосударственных конфликтов с уделением особого внимания следующим аспектам:

- определению, характеристикам и классификации информационных средств ведения боевых действий;
- определению и классификации информационного оружия и средств, которые могут быть использованы в качестве информационного оружия;
- разработке кодекса поведения применительно к информационному оружию;
- гарантиям равных прав для всех стран в отношении их самозащиты от кибератак;
- созданию глоссария Организации Объединенных Наций, содержащего определения основных терминов, связанных с информатизацией и телекоммуникациями в контексте международной безопасности.

Казахстан

[Подлинный текст на русском языке]
[2 июля 2009 года]

1. Активное развитие мировых информационно-коммуникационных технологий обусловливает глобальные преобразования во всех сферах жизни в любой стране. Как отмечается в Хартии глобального информационного общества (Окинава), «информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества».

2. В современных условиях роста научно-технического прогресса четко выделяется тенденция компьютеризации, создания разветвленных систем обработки данных. Интернет затрагивает практически все стороны государственной и общественной жизни, число его пользователей постоянно растет. В этом случае информационные ресурсы, системы обработки данных и компьютерные сети становятся самым уязвимым звеном национальной инфраструктуры государства.

3. С учетом того, что Интернет по-прежнему остается виртуально свободным пространством, практически никем не контролируемым, возможности со-

временных информационных технологий пытаются активно использовать преступные сообщества. По оценкам экспертов Международной торговой палаты, число преступлений, совершаемых с использованием сети Интернет, растет пропорционально числу пользователей. По данным Интерпола, Интернет стал той сферой, где «преступность растет самыми быстрыми темпами на планете».

4. Данные преступления условно можно разделить на три категории:

a) универсальные государственные и общественные: представляющие угрозу национальной и общественной безопасности (призывы к свержению существующего строя, утере суверенитета и независимости, подрыву национальных интересов, пропаганда терроризма, шовинизма, ксенофобии, всех видов экстремизма, этнической, расовой, религиозной, гендерной и прочей дискриминации и т.п.);

b) универсальные гражданские: представляющие угрозу правам и свободам личности (покушение на права и свободы личности, компромат, давление на личность, дискредитация личности, распространение конфиденциальной информации, использование услуг связи Интернет за чужой счет, подделка документов, нарушение авторских прав и т.п.);

c) традиционные: представляющие угрозу нравственным и моральным устоям и приличиям (порнография, педофилия, другие виды сексуальных извращений, наркомания, алкоголизм и т.п.).

5. Факты появления такого рода информации демонстрируют несовершенство национальных законодательств в части регулирования правоотношений, возникающих в сети Интернет, и требуют нового наднационального подхода. На международном уровне до сих пор отсутствует единый нормативный подход к определению и оценке угроз в области международной информационной безопасности, а также возможных механизмов международной кооперации по их предотвращению. При этом до настоящего времени ни одна из выдвигаемых отдельными странами концепций международной безопасности в сфере информационных технологий не имеет универсального характера.

6. Причинами этого являются имеющийся технологический разрыв между наиболее развитыми и отсталыми странами, скрытые политические разногласия и противоположные подходы в оценке явлений и событий в информационном пространстве и ряд других факторов.

7. Имеющиеся международные документы уровня ООН и Европейских организаций (ОБСЕ) в качестве основных приоритетов рассматривают угрозы общекриминальной преступности и терроризма в сфере информационных технологий, оставляя без внимания возможности неправомерного использования достижений информационных технологий в качестве информационного оружия во время вооруженных конфликтов, доминирующего положения в информационном пространстве, угрожающего национальному суверенитету и идентичности, а также угрозы природного и техногенного характера на объектах национальных информационных инфраструктур.

8. Важным элементом защиты от подобных угроз могли бы стать не только договоренности с военно-политическими партнерами в сфере международной информационной безопасности, но и политико-правовые соглашения в области взаимного неприменения информационного оружия, совместных механизмов

минимизации негативных последствий вредоносного воздействия и восстановления национальных информационных инфраструктур и др.

9. Следует отметить, что подобная работа уже ведется с участием представителей Республики Казахстан в рамках Организации Договора о коллективной безопасности (ОДКБ) и Шанхайской организации сотрудничества (ШОС), где на экспертном уровне прорабатываются возможности заключения соответствующих межправительственных соглашений. В частности, во исполнение Плана действий государств — членов ШОС по обеспечению международной информационной безопасности, утвержденного решением Совета глав государств — членов ШОС в г. Бишкеке от 16 августа 2007 года, группой экспертов государств — членов ШОС по вопросам международной информационной безопасности, разработан проект межправительственного Соглашения о сотрудничестве в области обеспечения международной информационной безопасности. Соглашение было подписано 15 июня 2009 года в г. Екатеринбурге в ходе заседания Совета глав государств — членов ШОС.

10. Следует обратить внимание, что Соглашение не имеет аналогов в мировой практике и, в случае его подписания, будет иметь важное международное значение с учетом возможности присоединения к нему других государств.

11. Кроме того, в рамках ОДКБ действует Временная рабочая группа при Комитете секретарей советов безопасности Организации по вопросам информационной политики и безопасности. Группа разработала Программу совместных действий по формированию системы информационной безопасности государств — членов ОДКБ.

12. Государства — члены ОДКБ провели совместные оперативно-профилактические мероприятия в рамках операции «ПРОКСИ» на основе единого замысла по направлениям взаимодействия органов безопасности и внутренних дел (полиции).

13. Учитывая масштабный и трансграничный характер сети Интернет, предлагаем государствам — членам Организации Объединенных Наций разработать и принять Международную конвенцию об информационной безопасности, одним из основных блоков которой будет борьба с преступлениями с использованием сети Интернет.

14. Данный документ должен быть направлен на взаимовыгодное международное сотрудничество в области информационной безопасности и предотвращение появления негативных геополитических последствий мировой информатизации.

15. Кроме того, в рамках Конвенции необходимо предусмотреть организационные, технические, программные, социальные механизмы в области получения информации, пользования ею в целях защиты конституционного строя, суверенитета и территориальной целостности всех стран — членов Организации Объединенных Наций, политической, экономической и социальной стабильности, законности и правопорядка, а также механизмы, способные реализовать конституционные права и свободы человека и гражданина.

16. В национальном плане в Казахстане разработан законопроект «О внесении изменений и дополнений в некоторые законодательные акты Республики

Казахстан по вопросам информационно-коммуникационных сетей», который находится на рассмотрении Сената Парламента.

17. Названным законопроектом предполагается законодательное закрепление норм по регулированию распространения информации на территории Республики Казахстан посредством информационно-коммуникационных сетей.

18. Для укрепления информационной безопасности и содействия международному сотрудничеству в этой области основные усилия на национальном уровне предпринимаются органами национальной безопасности. На постоянной основе осуществляются мероприятия по выявлению и пресечению компьютерных преступлений на международном уровне.

19. Так, в 2008 году Комитетом национальной безопасности совместно с Федеральной службой безопасности России пресечена деятельность транснациональной организованной преступной группы из числа хакеров, вымогавших крупные денежные средства за прекращение распределенных атак типа «отказ в обслуживании» на сайты компаний, осуществляющих предпринимательскую деятельность посредством сети Интернет.

20. Результаты проводимых оперативно-розыскных мероприятий в данной сфере показывают о появлении новых способов совершения преступлений с использованием сети Интернет, таких как вымогательство, шантаж, трафик людей, сводничество, распространение информации, пропагандирующей порнографию, культ жестокости и насилия, терроризм и экстремизм.

21. К примеру, в 2008 году выявлено 45 фактов распространения порнографии, при этом необходимо отметить рост доступности детской порнографии в Интернете. Так, если в 2005–2006 годах выявлено по одному факту распространения детской порнографии, в 2007 году — 7, то в 2008 году — 14, в том числе 2 в казахстанском сегменте Интернета.

22. Необходимо отметить и то, что противодействие преступлениям в сфере информационной безопасности и высоких технологий не отвечает предъявляемым требованиям ввиду отсутствия законодательной базы, которая четко регламентировала бы вопросы обеспечения информационной безопасности.

23. Имеющиеся нормативные правовые акты в данной сфере требуют дальнейшего совершенствования с учетом реалий настоящего времени.

24. На наш взгляд, было бы правильным, основываясь на опыте передовых стран, модернизировать действующее уголовное законодательство в сторону ужесточения карательной практики за совершение преступлений рассматриваемой категории.

25. Кроме того, принимая во внимание трансграничность компьютерных преступлений, правоохранительным органам необходимо на постоянной основе расширять сферы оперативного взаимодействия для быстрого реагирования на Интернет атаки. Результаты взаимодействия правоохранительных органов Казахстана со специальными службами и правоохранительными органами зарубежных стран указывают на активизацию компьютерных атак из казахстанского сегмента сети Интернет. При этом потерпевшие стороны постоянно сталкиваются с проблемой оперативности при передаче информации о совершаемой атаке ввиду отсутствия в республике официальной службы, ответственной за прием и передачу сведений о компьютерных инцидентах в компетентные госу-

дарственные органы по примеру функционирующих в других странах Центров Интернет безопасности (т.н. CHRT).

26. В этой связи, как нам видится, имеется необходимость создания в правоохранительных органах отдельных специализированных подразделений по выявлению, пресечению и раскрытию преступлений в сфере информационной безопасности, оснащенных передовыми средствами, для противодействия рассматриваемым преступлениям.

27. Казахстан также представил свои кандидатуры в Группу правительственных экспертов, которая будет создана в соответствии с пунктом 4 резолюции Генеральной Ассамблеи 63/37 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

Ливан

[Подлинный текст на английском языке]
[22 мая 2009 года]

1. Ливан готовит новый закон, охватывающий сферу информационно-коммуникационных технологий, который находится в стадии окончательного утверждения Палатой депутатов; этот закон будет охватывать все соответствующие вопросы, включая безопасность, и все аспекты, связанные с информационными преступлениями.

2. Как только вышеупомянутый закон вступит в силу, Министерство телекоммуникаций начнет заниматься вопросами, относящимися к подпунктам (b), (c) и (d) [пункта 3 резолюции 63/37], наряду с другими соответствующими министерствами и ведомствами.

Литва

[Подлинный текст на английском языке]
[26 мая 2009 года]

1. Литва придает большое значение вопросам информационной безопасности как в рамках своей национальной, так и международной повестки дня. Вопрос кибербезопасности является важным элементом национальной безопасности.

2. Большое значение имеет сотрудничество на международном уровне в целях обеспечения защиты коммуникационных и информационных систем и повышения осведомленности общественности. Литва приветствует тот факт, что вопрос информационной безопасности привлекает все большее внимание в рамках повесток дня международных организаций, таких, как Организация Объединенных Наций, Европейский союз, Организация Североатлантического договора, Организация по безопасности и сотрудничеству в Европе; Литва активно участвует в их работе по данной тематике. Ведомственные структуры Литвы тесно сотрудничают со своими партнерами. С 1 июля 2004 года Литва является участницей Конвенции о киберпреступности Совета Европы.

3. Литва является одним из семи членов Организации Североатлантического договора, которые выступили инициаторами создания в Таллине, Эстония, Экспертного центра НАТО по совместной кибероборонe. 14 мая 2008 года этот центр получил статус Экспертного центра НАТО.

4. Решением Европейского парламента и Совета 11 марта 2005 года была принята многолетняя программа Сообщества «Более безопасный Интернет плюс», направленная на обеспечение безопасного использования Интернета и новых онлайновых технологий. Основная задача этой программы — повышать осведомленность общества о вопросах обеспечения более безопасного Интернета и линий экстренной помощи.

5. На Генеральной ассамблее Международной ассоциации линий экстренной помощи, проходившей в Дублине 28 и 29 мая 2008 года, литовская служба экстренной связи стала членом этой Ассоциации.

6. Что касается национального уровня, в 2000 году была проведена первая оценка состояния информационной инфраструктуры, что стало отправным пунктом комплексной работы по данному вопросу. Среди основных аспектов оценки был уровень понимания вопроса информационной безопасности, текущая политика и уровень киберзащиты государственных учреждений.

7. Решением правительства Республики Литва (№ 291, 14 марта 2001 года) на Министерство внутренних дел были возложены функции координатора по обеспечению безопасности использования информационных технологий в государственных учреждениях.

8. Был разработан и реализован ряд мер, направленных на обеспечение информационной безопасности, как это предусмотрено в государственной стратегии обеспечения безопасности информационных технологий (до 2004 года) и в государственной стратегии обеспечения безопасности в сфере электронной информации в государственных учреждениях (до 2008 года).

9. Указом премьер-министра Литвы от 17 июня 2008 года была сформирована межведомственная рабочая группа по вопросам кибербезопасности. 21 ноября 2008 года эта рабочая группа представила правительству доклад с предложениями и рекомендациями по повышению уровня кибербезопасности в Литве.

10. Правительство Литвы планирует в ближайшем будущем подготовить проект Закона о сетях электронной коммуникации и информационной безопасности, а также новую Стратегию обеспечения безопасности электронной информации в целях дальнейшего совершенствования возможностей государства в сфере информационной безопасности, и в частности в сфере киберзащиты. Среди целей вышеупомянутой стратегии следует назвать обеспечение эффективности институциональной структуры как основы защиты от кибератак, поддержание безопасности и надежности инфраструктуры по передаче данных, эффективную защиту критически важной информационной инфраструктуры от киберугроз, обеспечение строгого соблюдения установленных норм и требований посредством проведения ревизионных проверок второй и третьей стороной.

11. С 2005 года Национальное управление по регулированию в коммуникационной сфере проводило обзоры функционирования сетей электронной комму-

никации и проверку уровня информационной безопасности в целях выявления нерешенных вопросов. Это Управление осуществляет функции национальной Группы по экстренному реагированию в сфере компьютерных технологий.

12. Литовской национальной Группе по экстренному реагированию в сфере компьютерных технологий поручено содействовать обеспечению безопасности в области информационных технологий через предотвращение, отслеживание и урегулирование проблемных ситуаций в сфере информационной безопасности, а также распространение информации об угрозах в этой сфере. 30 сентября 2008 года был открыт новый веб-сайт www.cert.lt. 16 января 2009 года эта Группа получила статус члена сети аккредитованных представителей европейских групп реагирования на угрозы безопасности вычислительных систем и групп по экстренному реагированию в сфере компьютерных технологий.

13. Литва стремится к обеспечению того, чтобы международное сообщество неизменно уделяло большое внимание вопросам информационной безопасности и вело более активную работу по решению проблем в этой сфере. Литва настроена на активное участие в будущей работе международного сообщества по обеспечению более надежной информационной безопасности и готова оказывать содействие этой деятельности.

Мексика

[Подлинный текст на испанском языке]
[8 июня 2009 года]

1. Опасения в сфере безопасности связаны прежде всего с возможной уязвимостью информационных систем, применяемых для управления программами обороны стран, а также угрозой применения террористами информационных и телекоммуникационных технологий для совершения насильственных или разубеждающих акций.

2. В этой связи и будучи обеспокоена вопросами повышения безопасности телекоммуникаций в мире, Мексика приняла участие во Всемирной ассамблее по стандартизации электросвязи, состоявшейся в Южной Африке в октябре 2008 года, в ходе которой вместе с другими членами Межамериканской комиссии по электросвязи (СИТЕЛ) (Канада, Парагвай и Уругвай), она представила резолюцию, содержащую обращение к университетам принять активное участие в работе сессий Международного союза электросвязи в целях активизации его работы.

3. Кроме того, на региональном уровне Мексика выступила в роли заместителя председателя двадцатого заседания Постоянного руководящего комитета СИТЕЛ, в ходе которого она ознакомила государства региона с программой по борьбе с вредоносными вмешательствами в работу спутниковых систем, которая осуществляется федеральной комиссией по телекоммуникациям. В этой связи государства приняли решение провести пятую очередную сессию Ассамблеи СИТЕЛ в Мексике в первом квартале 2010 года.

4. В числе мероприятий, которые Мексика проводит в целях укрепления международной безопасности в сфере информатики и связи, можно отметить создание подразделения полиции по борьбе с киберпреступностью, которое по-

мимо принятия профилактических мер по борьбе с преступлениями, совершаемыми через Интернет и другие информационные каналы, также создало специальную структуру по предупреждению и пресечению преступлений в отношении несовершеннолетних.

Сербия

[Подлинный текст на английском языке]
[9 июня 2009 года]

1. Государствам необходимо укреплять свою систему правовых норм в сфере киберпространства, поскольку эта задача уже не ограничивается территорией одной страны, а лица и/или группы, занимающиеся подрывом и/или несанкционированным использованием информационных и телекоммуникационных систем, не всегда находятся в той же стране, где происходит сбой. Резолюция Организации Объединенных Наций является лишь первым шагом и твердой основой для сбалансированного, учитывающего рекомендации подхода к укреплению законодательных механизмов на международном уровне в целях повышения международной безопасности, с одной стороны, и обеспечения свободного потока информации — с другой.

2. Необходимы более суровые законы, прежде всего национальные, при этом они должны отвечать уровню подготовки и технических навыков пользователей. Следует также непрерывно повышать уровень знаний пользователей и создавать специализированные учреждения, которые будут заниматься планированием, организационной и надзорной деятельностью в отношении технического аспекта в данной области.

3. По результатам оценки соблюдения принципа информационной безопасности в сфере информатизации и телекоммуникационных систем было выявлено следующее:

Проблемы

- Ежедневное появление новых типов вирусных программ, угрожающих безопасности информационных и телекоммуникационных систем
- Многочисленные попытки нарушить работу официальных веб-сайтов Министерства обороны и Вооруженных сил Республики Сербия
- Распространение идей терроризма в Интернете

Процедуры по обеспечению безопасности и сотрудничество

- Применение соответствующего антивирусного программного обеспечения на всех уровнях использования информационных и телекоммуникационных систем в Министерстве обороны и в системе Вооруженных сил Республики Сербия
- Непрерывная защита против хакерских атак официальных Интернет-сайтов Министерства обороны и Вооруженных сил Республики Сербия; а также

• Участие в конференциях и семинарах, направленных на повышение осведомленности об угрозе киберпреступности и кибертерроризма

Рекомендации

Создание международного агентства, которому были бы поручены следующие задачи:

– оценка проблем защиты данных и телекоммуникационных каналов;

– отслеживание факторов возможных угроз в сфере международного кибертерроризма и киберпреступности;

– оценка проблем международной безопасности в сфере информатизации и телекоммуникационных систем, а также рекомендации в решении подобных проблем;

– разработка учебных программ, направленных на повышение осведомленности об угрозах, связанных с киберпреступностью и кибертерроризмом;

– обеспечение обмена знаниями и опытом на межправительственном уровне.

Таджикистан

[Подлинный текст на английском языке]
[20 мая 2009 года]

1. В настоящее время сфера телекоммуникаций считается одним из наиболее важных факторов развития экономики, а также обеспечения стабильности и безопасности любого государства.

2. Таджикистан создал все необходимые условия для развития телекоммуникационной сферы благодаря свободной конкуренции и режиму лицензирования различных операторов и провайдеров, а также благодаря появлению новых видов услуг.

3. Обеспечению безопасности функционирования информационной и телекоммуникационной инфраструктуры, повышению уровня защиты корпоративных информационных систем необходимо уделять особое внимание, и посредством этой деятельности препятствовать распространению идеологии терроризма, экстремизма и насилия.

4. Таджикистан готов оказывать поддержку в реализации вышеупомянутой инициативы и сотрудничать в деле развития системы международной информационной безопасности.

Таиланд

[Подлинный текст на английском языке]
[3 июня 2009 года]

Общая оценка вопросов информационной безопасности

1. Современный мир представляет собой информационное общество, в котором информационные технологии используются для того, чтобы сделать жизнь более удобной. Например, такие технологии используются для осуществления финансовых операций и обмена новостями и информацией. Однако эти технологии являются не только благом, они могут также использоваться определенными группами в незаконных и неблаговидных целях, что создает такие проблемы, как хищение информации из информационных систем, кибератаки, подделка электронных документов, проникновение в правительственные базы данных с целью похищения личной информации, а также нарушение принципа конфиденциальности. Тем не менее информационно-коммуникационные технологии необходимы для экономического развития каждой страны. Усложнение технологий, нехватка хорошо подготовленного персонала для обеспечения информационной безопасности, а также недостаток ресурсов могут привести к снижению уровня информационной безопасности компьютерных систем и сетей, что в свою очередь чревато потерей доверия со стороны общества, прежде всего к банковской сфере, электронной торговле и системе управления. Поэтому необходимо выявлять и прогнозировать возможные сопутствующие проблемы и создавать систему гарантий и мер безопасности для защиты от подобных рисков. Для этого странам следует совместно разрабатывать меры информационной безопасности, с тем чтобы обеспечить наличие международных стандартов, которым бы следовали все страны.

Усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в данной сфере

2. Правительство Королевства Таиланд включило политику обеспечения безопасности в число приоритетов правительственного стратегического плана на 2552–2554 годы Эры Будды (2009–2011 годы). В настоящее время правительство реализует законодательные меры для повышения уровня информационной безопасности, с тем чтобы предотвратить использование информационных сетей в неблаговидных целях и устранить угрозу национальной безопасности. Подобные меры включают в себя законы о преступлениях в компьютерной сфере, об электронных трансакциях, электронных подписях и электронных переводах денег.

3. Министерство информации и коммуникационных технологий придает большое значение обеспечению информационной безопасности сетей Интернет, решению проблемы существования нелегальных веб-сайтов и веб-сайтов с сомнительным содержанием; с этой целью был создан оперативный центр по обеспечению безопасности Интернета, в задачи которого входит отслеживание угроз в сфере информационных технологий, а также обеспечение координации с другими учреждениями применительно к использованию информационных сетей как источника угрозы национальной безопасности. Еще одной целью этого оперативного центра является решение проблемы нелегального исполь-

зования информационных сетей и создание системы отслеживания источников вирусов и электронного «мусора».

4. На международном уровне необходимо создать координационный орган, который мог бы выполнять функции контактного центра. Этот орган должен разрабатывать стратегии по предотвращению и прекращению распространения информации ненадлежащего характера, а также определять меры борьбы с угрозами информационной безопасности. Также необходима система превентивных мер, которые могли бы служить руководящими принципами для совместных действий.

Анализ соответствующих международных концепций по повышению уровня безопасности глобальных информационных и телекоммуникационных систем

5. Нынешний кибернетический мир является взаимосвязанным и не имеет границ, поэтому необходимо сформировать общие международные концепции и принципы содействия глобальной информационной безопасности. Проблемы информационной безопасности, возникающие в одной стране, могут распространяться за ее пределы и повлиять на другую страну.

Меры, которые может предпринять международное сообщество для повышения уровня информационной безопасности на глобальном уровне

6. Меры, которые могло бы предпринять международное сообщество, включают обмен информацией, совместные превентивные меры и способы борьбы с угрозами информационной безопасности. Также следует развивать сотрудничество, направленное на расширение возможностей в сфере информационных технологий различных стран, и тем самым обеспечивать равный уровень, прежде всего за счет передачи технологий и специальных знаний развитых стран менее развитым странам, с тем чтобы последние могли укрепить свой потенциал. Также необходимо разработать учебные программы, охватывающие вопросы осведомленности, предотвращения, выявления, управления и реагирования, с тем чтобы минимизировать уровень рисков и угроз информационной безопасности.

7. Помимо этого, необходимо создать координационный механизм для обеспечения взаимосвязи между работой различных соответствующих учреждений и задать направление и определить политику, которая позволила бы закрепить определенный стандарт национальной информационной безопасности и обеспечить однонаправленность действий.

8. Следует поощрять усилия ряда международных учреждений по расширению международного сотрудничества в деле повышения информационной безопасности, прежде всего это касается Международного союза электросвязи (МСЭ). МСЭ организовал международную конференцию по обмену опытом и разработке мер для решения проблем, связанных с ненадлежащим использованием информационных технологий. МСЭ также создал аналитические группы, которым поручено определить меры повышения информационной безопасности, которыми могли бы пользоваться правительства и соответствующие учреждения.

9. Также в каждой стране следует создать группы по экстренному реагированию в сфере компьютерных технологий при содействии стран, которые с успехом сформировали такие группы.

10. Помимо этого, следует заняться вопросом защиты от кибератак критически важной для каждой страны инфраструктуры и сформировать систему быстрой помощи или сотрудничества в рамках международного сообщества, а также совместно изучить возможные пути устранения или минимизации подобных рисков.

11. Следует обеспечивать более высокий уровень осведомленности о проблеме информационной безопасности в рамках Организации Объединенных Наций, в связи с чем можно было бы организовать дискуссию для определения возможных правил и положений, касающихся информационных войн, а также обсудить идею выпуска ежегодных докладов об угрозах и возможных проблемах в сфере информационной безопасности.

Украина

[Подлинный текст на русском языке]
[20 мая 2009 года]

1. Интерес к проблемам информационной безопасности определяется все возрастающей ролью информации в различных сферах жизнедеятельности общества. С внедрением в повседневную жизнь государства и общества передовых информационных технологий, расширяются возможности воздействия информационных угроз на информационно-телекоммуникационные системы, информационные ресурсы государственных органов и коммерческих структур со стороны криминального мира и отдельных лиц, с целью совершения противоправных действий.

2. Половина зафиксированных компьютерных преступлений в мире относится к несанкционированному доступу к компьютерной информации. Растет корыстная направленность компьютерных преступлений вместе с нанесенным материальным ущербом. В настоящее время возросло количество преступлений, совершенных транснациональными хакерскими группами.

3. Компьютерная преступность характеризуется высокой латентностью, восстановление полной картины правонарушения становится невозможным по причине того, что как государственные, так и коммерческие структуры, подвергшиеся компьютерным атакам, всячески стараются скрыть такие факты, боясь потерять авторитет, не склонны афишировать нанесенный ущерб и слабую систему защиты информации. Вследствие этого случаи таких преступлений становятся достоянием гласности далеко не всегда, что говорит о необходимости развития совместных мер профилактического и предупредительного характера, которые должны быть основополагающими в системе защиты информации.

4. Компьютерные преступления, как правило, становятся лишь первым шагом в цепочке криминальных деяний, направленных на другие традиционные виды преступления — хищения, вымогательство, мошенничество и так далее. С каждым днем преступления становятся более совершенными, изо-

щренными и скрытными, наносящими огромный экономический и политический ущерб практически всем странам мира. Кроме того, большинство экспертов напрямую связывают информационный суверенитет государства с вопросами национальной безопасности.

5. В ходе борьбы с преступлениями в сфере информационных технологий возникают многочисленные проблемы правового характера, вызванные нематериальностью, а зачастую и недолговечностью электронных улик. Сложность разрешения проблем, характерных для кибернетической преступности, делает особенно актуальным международное сотрудничество, для чего все страны должны, в конечном счете, располагать соответствующими и совместимыми между собой правовыми, процессуальными и нормативными средствами.

6. Практика расследования компьютерных преступлений приводит к необходимости налаживания взаимодействия между правоохранительными органами различных государств.

7. В мире существует практика проведения совместных мероприятий при проведении расследований компьютерных преступлений. Служба безопасности Украины принимает активное участие в совместных операциях правоохранительных органов и специальных служб мира, проводимых в рамках борьбы с детской порнографией, мошеннических действий в сети Интернет, международным терроризмом.

8. Кроме того, необходима консолидация усилий по дальнейшему развитию сотрудничества в области обеспечения информационной безопасности, совпадающих интересов и проведение мероприятий по их защите, преимущественно на основе двухсторонних и многосторонних договоров. Успешное решение проблем информационной безопасности, на наш взгляд, возможно лишь при эффективном взаимодействии государственных структур различных государств, тем более что необходимая правовая база уже имеется.

9. С учетом необходимости противодействия угрозам кибернетической преступности и кибертерроризму, Служба безопасности Украины поддерживает контакты с правоохранительными органами и специальными службами иностранных государств.

10. Следует отметить, что нередко объектами нападений киберпреступников становятся сети государственных учреждений и от качественности установленных международных связей, а также оптимизации национальных законодательств под современные условия зависит успех по розыску и наказанию преступников.

11. Во взаимодействии с Национальной полицией Королевства Нидерландов и Федеральной службой безопасности России в конце 2008 года проведена скоординированная операция по пресечению противоправной деятельности международной преступной хакерской группировки, которая занималась хищением денежных средств клиентов финансово-кредитных учреждений путем несанкционированного вмешательства в работу их автоматизированных систем.

12. Принимая во внимание постоянный рост компьютерной преступности в мире, существование связи между хакерскими преступными группиров-

ками разных стран, независимости кибернетических угроз от государственных границ, постоянно расширять международное сотрудничество в сфере противодействия киберугрозам.

13. Так, в соответствии с международной Конвенцией о киберпреступности создан вполне жизнеспособный и удобный механизм — сеть национальных контактных пунктов «24/7», — который объединяет страны большой восьмерки и иные государства участники Конвенции.

14. В соответствии с решением Президента Украины о создании на базе Службы безопасности Украины национального контактного пункта «24/7», межведомственная рабочая группа из числа сотрудников Службы безопасности, Министерства внутренних дел, Генеральной прокуратуры и Министерства юстиции Украины разрабатывает проекты Законов Украины «О внесении изменений к Закону Украины «О ратификации Конвенции о киберпреступности», «О внесении изменений к Закону Украины «О телекоммуникации», «О структуре и общей численности Службы безопасности Украины», а также Указа Президента Украины об организации работы указанного контактного пункта.

15. В настоящее время в рамках выполнения решения Президента Украины Службой безопасности Украины осуществляются шаги по регистрации национального контактного пункта в международной сети.

16. Предполагается, что в результате работы в Украине указанного контактного пункта будут еще более оперативно и качественно решаться задачи по обмену информацией и противодействию киберугрозам в международном масштабе.

17. С целью реализации решений Всемирной встречи на высшем уровне по вопросам информационного общества (первый этап — Женева, 10–12 декабря 2003 года, второй этап — Тунис, 16–18 ноября 2005 года) в Украине был принят Закон «Про основные принципы развития информационного сообщества в Украине на 2007–2015 года», основными приоритетами которого является интеграция в глобальное информационное пространство и развитие информационного сообщества. Данным законом предусмотрено улучшение состояния информационной безопасности в условиях использования новейших ИКТ.

18. Кроме того, разработана и принята Конвенция развития телекоммуникаций в Украине, в которой предусмотрено проведение организационно-технических мероприятий, направленных на обеспечение безопасности функционирования всех элементов телекоммуникационной инфраструктуры Украины, а именно:

– создание и постепенное внедрение нормативно-правовой базы с обеспечением вопросов технической и криптографической защиты информации, гармонизированного с европейскими и международными стандартами;

– разработка современных методов защиты информации на базе технических средств для комплексного решения задач обеспечения защиты информации в телекоммуникационных сетях;

– создание системы легального перехвата информации в телекоммуникационных сетях в случаях, предусмотренных законодательством;

– создание государственного координационного центра по вопросам безопасности в информационно-телекоммуникационных сетях общественного пользования, содействие созданию государственных и негосударственных центров компетенции и реагирования на инциденты в телекоммуникационных сетях.

19. Нормативно-правовую базу защиты информации в Украине также составляют Законы Украины «Об основах национальной безопасности Украины», «Об информации», «О защите информации в информационно-телекоммуникационных системах» (далее — Закон), акты Президента и Кабинета Министров Украины «Положение о технической защите информации в Украине», «Правила обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах» (далее — Правила), «Порядок подключения к глобальным сетям передачи данных» и ряд других, а также значительное количество зарегистрированных в Министерстве юстиции нормативных актов, регламентирующих вопросы подключения информационных систем к глобальным сетям, лицензирования отдельных видов деятельности, порядок проведения оценки продукции в сфере защиты информации и другие.

20. Нормативно-правовыми актами определено, что для обработки подлежащей защите информации должны использоваться только защищенные информационно-телекоммуникационные системы (далее — ИТС), т.е. такие, в которых создана комплексная система защиты информации (далее — КСЗИ) как единая совокупность правовых и организационных мероприятий, а также программно-технических средств, способных противодействовать угрозам. При этом КСЗИ, а также используемые в ее составе средства защиты должны иметь подтверждение своего соответствия требованиям нормативных документов в области защиты информации.

21. С целью нормирования требований к КСЗИ и отдельным средствам защиты информации в Украине разработаны и введены в действие около 50 нормативных документов технического характера, устанавливающих критерии оценки защищенности информации, классификацию ИТС, порядок выполнения работ по защите, требования к отдельным средствам защиты и КСЗИ, в зависимости от класса ИТС, назначения, области применения, вида обрабатываемой информации.

22. Также в Украине создана собственная национальная система критериев оценки защищенности информационных технологий. Система базируется на комплексе нормативных документов по защите информации в ИТС от несанкционированного доступа, которые гармонизированы с аналогичными документами стран ЕС и международными стандартами, в частности со стандартом 15408 Международной организации по стандартизации/Международной электротехнической комиссии.

23. Кроме того, в Украине на национальном уровне создается система организационно-технических мер, направленная на противодействие осуществлению несанкционированных действий в отношении информационно-телекоммуникационных систем органов государственной власти, правоохранительных, таможенных, налоговых органов, учреждений кредитно-финансовой сферы, и других, в частности попыткам вмешательства в их работу с использованием возможностей глобальной сети Интернет.

24. Мировое сообщество отреагировало на такие действия созданием развитой и распределенной системы структур быстрого реагирования на инциденты, которые угрожают безопасности информационных ресурсов — группы реагирования на чрезвычайные происшествия в компьютерной сфере (computer emergency response team). Координацию действий таких структур на международном уровне осуществляет международная организация "Forum for incident response security teams" — форум реагирования на инциденты безопасности.

25. С целью создания нормативно-правового обеспечения подобной деятельности Администрацией Госспецсвязи был издан приказ от 10 июня 2008 года № 94 «Об утверждении порядка координации органов государственной власти, органов местного самоуправления, военных формирований, предприятий, учреждений, организаций независимо от форм собственности по вопросам предотвращения, выявления и ликвидации последствий несанкционированных действий в отношении государственных информационных ресурсов в информационных, телекоммуникационных и информационно-телекоммуникационных системах».

26. В рамках реализации данного приказа была создана соответствующая веб-страница и почтовый адрес в сети Интернет (www.cert.gov.ua).

27. В Украине, используя международный опыт обеспечения безопасности информационных ресурсов, осуществляются мероприятия по созданию на базе Госспецсвязи национального координатора по предотвращению совершения нарушений безопасности информации в ИТС (группы по реагированию на чрезвычайные происшествия в компьютерной сфере Украины (CERT-Ukraine)) и его аккредитация в Форуме реагирования на инциденты безопасности. С этой целью 17 марта 2009 года организована и проведена встреча представителей Администрации Госспецсвязи и старшего советника по вопросам информационной безопасности Уполномоченного органа Финляндии по регулированию телекоммуникаций.

28. Несмотря на отсутствие аккредитации CERT-Ukraine в Форуме реагирования на инциденты безопасности, украинской стороной в течение 2006–2008 годов было получено более 200 сообщений от группы реагирования на чрезвычайные ситуации в компьютерной сфере в Финляндии, Австралии, Австрии, Словении и других государств о несанкционированных действиях в глобальной сети Интернет со стороны украинских пользователей. По результатам предпринятых действий в адреса соответствующих Интернет Провайдеров было направлено более 250 электронных писем с целью принятия мер по локализации источников вредоносного программного обеспечения и вирусов. Также, в мае 2007 года осуществлялись мероприятия по прекращению DDoS-атак на эстонские сервера, источники которой находились в Украине, а в октябре 2007 года была прекращена DDoS-атака на веб-сайт Президента Украины.

29. Необходимо добавить, что в Украине созданы нормативно-правовые основы и организована работа по обеспечению взаимодействия Госспецсвязи и правоохранительных органов, направленная на реализацию мероприятий по обеспечению безопасности государственных информационных ресурсов в ИТС и повышение эффективности системы реагирования на несанкционированные действия в отношении указанных информационных ресурсов.

30. Таким образом, сегодня в Украине обеспечена возможность выполнения работ по защите информации на всех этапах создания ИТС и КСЗИ в ИТС, независимо от вида и критичности обрабатываемой информации, вида и сложности ИТС. При этом все основные подходы к формированию требований, проектированию, разработке, оценке защищенности и обеспечению защиты информационных ресурсов в ИТС в целом совпадают с подходами, применяемыми ответственными за безопасность государственными органами стран — членов Организации Объединенных Наций и ЕС.

31. С целью проведения образовательной деятельности по подготовке специалистов в сфере информационной безопасности и компьютерной инженерии на базе Государственного университета информационно-коммуникационных технологий создан Институт защиты информации, являющийся учебным и научным структурным подразделением Университета.