УДК 39.727.22/24:338.47

МЕЖДУНАРОДНЫЙ ФОРМАТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.А. Сейдакматов

Раскрывается актуальность международной информационной безопасности, а также пути решения этих проблем.

Ключевые слова: национальный форум; безопасность информации; информационные и телекоммуникационные технологии (ИКТ).

На 10-м январском Национальном форуме информационной безопасности был создан международный оргкомитет Евразийского форума, сопредседателями которого стали председатели профильных комитетов (комиссий) парламентов Казахстана, Беларуси и России, а также заместитель Генерального секретаря ОДКБ.

Ежегодно в мероприятиях форума принимает участие более двух тысяч специалистов из разных регионов России и стран ближнего и дальнего зарубежья.

В качестве основных задач проведения мероприятий форума является развитие контактов между государственными органами и негосударственными организациями, специалистами, работающими в сфере информационной безопасности, создание условий для свободного обмена передовыми идеями и опытом в сфере развития информационного общества и обеспечения информационной безопасности, включая формирование нормативной правовой базы.

Это свидетельствует в первую очередь об актуальности обсуждения проблем информационной безопасности именно в международном формате. Ведь все мы, хотим того или нет, уже давно находимся на “информационной планете”, не имеющей

привычных государственных границ в информационном пространстве. На этой планете живут люди всех возрастов, рас, полов, вероисповеданий, с удовольствием использующие новейшие информационные и коммуникационные технологии для личных и общественных целей, во благо и во вред.

Неизбежность и целесообразность использования информационных технологий и глобальных коммуникаций влечет за собой неотвратимость угроз информационной безопасности. Каждый из нас, любое ведомство, страна и мировое сообщество сталкиваются с этими угрозами и не осознавать это опасно. Потеря информации в личном компьютере в результате проникновения вируса ощутима для его владельца, но нарушение работы систем государственного управления, систем жизнеобеспечения задевает интересы общества, национальные интересы в целом [1].

Надо отдавать себе отчет в том, что в настоящее время угрозу информационной безопасности реализуют не только или не столько хакеры. Соответствующие технологии широко используются в конкурентной борьбе, а также военными организациями и спецслужбами всех стран.

Масштабность угроз информационной безопасности, осознанная международным сообществом, нашла отражение в документах Всемирной встречи на высшем уровне по вопросам информационного общества, где содержится призыв ко всем участникам информационного общества предпринимать соответствующие действия и принимать установленные законодательством меры по предотвращению ненадлежащего использования информационных и телекоммуникационных технологий (ИКТ).

Информационная грамотность, включающая в себя и навыки культуры кибербезопасности, становится важнейшим фактором создания информационного общества как общества знаний. Эта позиция ЮНЕСКО поддержана участниками Глобального альянса по информационным технологиям и развитию ООН.

Сложность противодействия угрозам информационной безопасности определяется характером проблемы.

Во-первых, угрозы глобальны, они касаются каждого, поскольку все мы имеем дело с информацией. Пока еще только около 20 % жителей Кыргызстана пользуются Интернетом, но это число интенсивно растет и в самое ближайшее время можно ожидать, что половина населения почуствует остроту угроз информационной безопасности.

Во-вторых, эти угрозы трансграничны, что существенно затрудняет организацию противодействия, поскольку требует объединения регламентированных правовыми документами усилий различных стран. Не всегда такие документы есть.

В третьих, способы реализации угроз информационной безопасности и формы их проявления постоянно совершенствуются, а система противодействия фактически только реагирует на известные угрозы и постфактум ищет способы их отражения.

Наконец, высокая технологичность этих угроз требует адекватных мер противодействия, предъявляет требования к квалификации специалистов по информационной безопасности, материально-техническому и кадровому обеспечению правоохранительных органов и спецслужб.

Жизнь любого социума даже на “информационной планете” невозможна без выработки правил общежития. Глобальная инфраструктура этой жизни завязана на Интернете. Он возник как саморегулирующаяся система, в которой прежде всего применяются технические нормы и правила, позволяющие беспрепятственно устанавливать связи между пользователями, обеспечивать доступ и передачу информации.

Интернет несет обществу иные потенциальные угрозы, являющиеся, как водится, обратной стороной его преимуществ:

- отсутствие общепризнанных правил поведения, имеющих обязательную силу и обеспечивающих участникам “сетевых” отношений защиту чести, достоинства, деловой репутации, неприкосновенности частной жизни, общественной нравственности, запрет пропаганды антиобщественного поведения, насилия, в частности распространения информации о способах совершения террористических актов;
- возможность проникновения в автоматизированные системы, обеспечивающие жизнедеятельность общества, создает угрозу не только нарушения нормальной работы этих систем, но и угрозу жизни людей;
- возможность анонимного присутствия в сети позволяет распространять ложную информацию, не боясь справедливого наказания; сложность выявления правонарушителя и сбора доказательств затрудняет свершение правосудия;
- отсутствие системы общественного контроля и самоцензуры приводит к тому, что доверие к предоставляемой в сети информации снижается [2].

По мере развития сети и формирования киберсообщества возникла необходимость во внедрении социальных норм, регулирующих отношения между людьми, и прежде всего норм права.

Но оказалось, что они труднореализуемы. Кроме того, новые инфокоммуникационные технологии совершенствуются так быстро, что развитие права и законодательства заметно отстает. Традиционные представления о территориальной юрисдикции, административных границах и т. п. применительно к киберпространству во многом вообще теряют смысл. Роль национального законодательства снижается. На первый план выходят инструменты межгосударственного (международного) регулирования [3].

Общество идет по этому пути, вырабатывая принципы и формы взаимодействия в глобальном информационном пространстве. Были приняты Европейская конвенция по преступности в сфере компьютерной информации (ETS № 185) и Дополнительный протокол к этой конвенции относительно введения уголовной ответсвенности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (ETS № 189). Руководством нашей страны было принято решение о ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информации (1 июня 2001 г.).

В течение прошлых лет были приняты важные решения в рамках Содружества независимых Государств, направленные на организацию сотрудничества в области обеспечения информационной безопасности стран-участниц и Содружества в целом. Так, Экономический совет СНГ принял Решение о деятельности регионального содружества в области связи (14 декабря 2007 г.). Совет глав государств СНГ 5 октября 2007 г. утвердил Межгосударственную программу совместных мер борьбы с преступностью и программу Сотрудничества государств-участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма, предусматривающих активизацию информационного взаимодействия и сотрудничества в борьбе с этим злом XXI в., создание специализированного банка данных, пресечение информационно-пропагандистской деятельности террористических организаций.

Здесь на помощь приходит и киберсообщество, которое делает попытку организовать саморегулирование не только в технической, но и в "социальной" составляющей жизни в глобальном пространстве. В последнее время получила широкое обсуждение идея организации "горячей линии" для противодействия распространению в сети Интернет незаконной информации. Такие "горячие линии" есть уже в 21 стране мира. Их взаимодействие позволит в какой-то степени нейтрализовать проблему экстерриториальности Интернета, что нам представляется весьма актуальным.

Концепция дальнейшего развития Содружества Независимых Государств, одобренная Советом глав государств 5 октября 2007 г., особое внимание уделяет предупреждению терроризма, противодействию его идеологии и пропаганде и ориентирована на сотрудничество в сфере безопасности, борьбы с преступностью, поддержания и укрепления международной безопасности и стабильности, противодействия новым вызовам и угрозам, в том числе в сфере применения информационных технологий.

С развитием технологий проблемы информационной безопасности видоизменяются и наращиваются. Наряду с вечной проблемой защиты конфиденциальной информации, перед сообществом встает в полный рост проблема защиты открытых веб-сайтов, содержащих необходимую и полезную информацию. Атакам вандалов подвергаются как сайты органов государственной власти, так и социальные сети и проекты [4].

Большую проблему для бизнеса в сети и поиска правонарушителей составляет персонификация пользователей. Свобода провоцирует мошенничество, различные формы которого встречаются в Сети все чаще. Поэтому в будущем, полагают аналитики, авторизация пользователей для проведения транзакций через Интернет должна стать обязательной. Механизмы и границы ограничения анонимности в Сети должны вырабатываться в диалоге власти с киберсообществом.

Эти вопросы связаны и со статусом так называемых сервис-провайдеров или провайдеров контента, которые, наряду с автором, должны отвечать за информацию, размещенную на их оборудовании.

Возникновение новых вызовов и угроз информационной безопасности, изменение приоритетов позволяет ставить вопрос о скорейшем принятии Закона "Об информационной безопасности Кыргызской Республики", с акцентом повышения эффективности государственной системы обеспечения информационной безопасности в различных ее областях, системности мер поддержки кыргызстанских производителей информационных технологий (в том числе технологий информационной безопасности) и др. [5].

Состояние информационной безопасности в нашей республике характеризуется высоким уровнем технологической зависимости. Это касается как технических средств, так и программного обеспечения, в первую очередь системного. Такая

зависимость в некоторых секторах государственного управления может создать угрозу национальной безопасности. Эта проблема осознается ведущими странами Европы и Азии, которые ищут альтернативу в разработке национальных программных продуктов на основе систем с открытым кодом [6].

Руководство страны принимает активные меры в принятии национальной программы борьбы с коррупцией. Информационные технологии могут и должны прийти на помощь такой программе. Прежде всего это касается информационной открытости органов государственной власти и органов местного самоуправления, прозрачности процедур государственного управления, представления для общего доступа максимального объема информации, затрагивающей права, свободы и обязанности человека и гражданина. [7]

Литература

1. Закон КР "Об утверждении положения об обеспечении безопасности персональных данных при их обработке" № 781 от 17 ноября 2007 г.
2. Приказ "Об утверждении Положения о ведении реестра операторов, осуществляющих обработку персональных данных" № 154 от 28 апреля 2008 г.
3. *Карпов В.И.* Основы теории обеспечения безопасности личности, общества и государства: учебн. пособие / В.И. Карпов, Д.Б. Павлов. М.: Юридический институт МГУ путей сообщения (МИИТа), 2000. 139 с.
4. *Темирбаев К.Т.* Информационная безопасность Кыргызской Республики / К.Т. Темирбаев, А.А. Сагымбаев, Р.Н. Джаркеев. Бишкек, 2007. 114 с.
5. Проблемы национальной безопасности Кыргызстана. Бишкек: Институт социально-политических технологий, 2006. 341 с.
6. Концепция национальной безопасности Кыргызской Республики от 18 февраля 2009 г. Бишкек, 2009.