МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО УКРАИНЫ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Виктор КЛОЧКО,
соискатель кафедры общеправовых дисциплин
факультета права и массовых коммуникаций
Харьковского национального университета внутренних дел

Summary

The article is devoted to the research of the priorities of Ukraine's international cooperation in the field of information security in the terms of integration process. The main problems and threats to Ukraine's information security guaranteeing at the international level are defined. The notions of "information security", "international information security" and "international cooperation in the field of information security" are revealed. The author analyzes international experience of information security guaranteeing. On the basis of conducted study some propositions concerning the main directions of improving the national legislation in the field of information security guaranteeing and the need for implementation of international legal instruments are grounded.

Key words: information, international information security, information and communication technologies, international and legal regulation, international cooperation, information security policy.

Аннотация

Статья посвящена исследованию приоритетных направлений международного сотрудничества Украины в сфере информационной безопасности в условиях интеграционных процессов. Определены проблемы и угрозы обеспечения информационной безопасности Украины на международном уровне. Раскрываются понятия «информационная безопасность», «международная информационная безопасность» и «международное сотрудничество в сфере информационной безопасности». Проводится анализ международного опыта обеспечения информационной безопасности. На основе проведенного исследования обосновываются предложения относительно основных направлений усовершенствования национального законодательства в сфере обеспечения информационной безопасности, а также необходимости имплементации норм международно-правовых актов.

Ключевые слова: информация, международная информационная безопасность, информационно-коммуникационные технологии, международно-правовое регулирование, международное сотрудничество, политика информационной безопасности.

Постановка проблемы. Проблема обеспечения национальной безопасности в информационной сфере пока что находится на стадии разработки. Это обстоятельство обуславливается неадекватностью связи между формированием информационной цивилизации и мерами по обеспечению информационной безопасности. В связи с этим возникает проблема относительно формирования подходов по выработке концептуального видения информационной безопасности и ее места в системе национальной безопасности Украины.

Обеспечение информационной безопасности связано с одной из характерных особенностей современного этапа мирового научно-технического прогресса – глобальной информационной революцией, в результате которой происходит чрезвычайно быстрое и практически повсеместное распространение новейших информационных технологий и глобальных средств коммуникации, формируется своего рода глобальное информационное пространство международного сообщества. Использование достижений в информационной сфере возможно не только в позитивных целях, но и в целях, связанных с обеспечением превосходства отдельных государств на международной арене, с подавлением других государств, вмешательством во внутренние дела государства. В связи с этим все большее значение приобретает развитие сферы международного противоборства, затрагивающей как интересы безопасности Украины, так и общую систему международной безопасности на глобальном и региональном уровнях. Именно поэтому проблема информационной безопасности является актуальной в настоящее время.

Состояние исследования. Изучением проблем международной информационной безопасности относительно современных концепций международной безопасности, международной безопасности через сотрудничество, информационной безопасности в массово-коммуникационной сфере занимались такие отечественные ученые, как О.В. Бойченко, А.Г. Белорус, В.А. Липкан, В.Н. Лопатин, Д.Г. Лукьяненко, Е.А. Макаренко, А.М. Гуз. В зарубежных странах, например США, Великобритании, Швейцарии, вопросы информационной безопасности разрабатывались в трудах таких ученых, как Р. Моландер, С. Сьянг, Л. Борг, С. Хамфрефорс, Э. Ратмелл, Р. Старк, Р. Хандли, Р. Андерсен, Р. Харкнетт, А. Коэтзи, Х. Бэй, Э. Риддиле, П. Вилсон, Дж. Арквилла, Д. Ронфельдт, Д. Гомперт и другие.

Комплексные исследования проблем и перспектив развития эффективного механизма обеспечения международной информационной безопасности относительно вопросов международных отношений государств до настоящего времени не проводились. Необходимость дальнейшего научного исследования проблем и перспектив обеспечения международной информационной безопасности обосновывает также высокая динамика развития международных отношений при стремительном развитии информационно-телекоммуникационных систем и технологий.

Целью работы является комплексное изучение проблем, связанных с вопросами международного сотрудничества Украины в сфере информационной безопасности, а также разработка предложений по развитию системы обеспечения международ-

ной информационной безопасности, основой которой является не только разработка соответствующих международных нормативно-правовых актов, но и создание действующего механизма обеспечения информационной безопасности Украины на международном уровне.

Изложение основного материала. В 2001 г. Европейской Комиссией был представлен первый документ под названием «Сетевая и информационная безопасность: европейский политический подход» (Network and Information Security: Proposal for A European Policy Approach), в котором отражается европейский подход к проблеме информационной безопасности. В нем используется термин «сетевая и информационная безопасность», который трактуется как способность сети или информационной системы сопротивляться случайным событиям или умышленным действиям, которые представляют угрозу доступности, подлинности, целостности и конфиденциальности хранящихся или передающихся данных, а также услуг, предоставляемых через эти сети и системы [1].

Европейское сообщество отмечает, что сетевая и информационная безопасность становится ключевым фактором в развитии информационного общества. Прежде всего, сети и информационные системы содержат конфиденциальные данные и экономически ценную информацию, что повышает стимул для атак. Атаки на информационные системы могут иметь серьезные в национальном масштабе последствия, например, сбои в работе систем коммуникаций, утечку конфиденциальной информации.

Проблема заключается в том, что точно оценить масштаб фактических и потенциальных убытков вследствие нарушения сетевой безопасности очень трудно, поскольку, во-первых, нет системы оповещения, а во-вторых, атаки вызывают значительное количество нематериальных убытков, в том числе для репутации, поэтому многие кампании стараются не информировать о таких событиях, боясь негативной рекламы. К тому же сетевая и информационная безопасность являются динамичной проблемой. Быстрое технологическое развитие постоянно создает новые вызовы и угрозы, требует новых решений. В названном выше документе определены следующие основные направления европейской политики информационной безопасности:

– увеличение осведомленности пользователей о возможных угрозах при пользовании коммуникационными сетями;

– создание европейской системы предупреждения и информирования о новых угрозах;

– обеспечение технической поддержки;

– использование единой системы стандартизации и сертификации;

– правовое обеспечение;

– укрепление безопасности на государственном уровне;

– развитие международного сотрудничества.

На сегодняшний день Европейская Комиссия принимает участие в работе «Большой восьмерки», Организации экономического сотрудничества и развития и ООН. Частный сектор работает над проблемами безопасности в таких организациях, как Глобальный бизнес-диалог (www.GBDe.org) или Глобальный интернет-проект (www.GIP.org).

10 марта 2004 г. было создано Европейское агентство по сетевой и информационной безопасности (European Network and Information Security Agency). Европейское агентство по сетевой и информационной безопасности – это агентство Европейского Союза (далее – ЕС), созданное с целью повышения эффективности функционирования внутреннего рынка. Агентство выступает в роли консультанта и центра передовых технологий в сфере сетевой и информационной безопасности для стран-членов и институтов ЕС. Кроме того, агентство содействует развитию связей между странами-членами ЕС, институтами ЕС, хозяйствующими субъектами и частным бизнесом [2].

Политические приоритеты в сфере информационной безопасности, определенные руководящими органами ЕС, воплощаются в жизнь на национальном уровне как органами государственной власти, так и неправительственными организациями.

Одной из стран-лидеров ЕС по показателям развития информационного общества является Финляндия. В рейтинге стран ЕС Финляндия занимает первое место по уровню цифровой грамотности (более 50% населения), второе место – по показателю распространения сети широкополосной связи (34% населения) [3].

Основными государственными учреждениями, ответственными за разработку и реализацию политики информационной безопасности, в Финляндии является Министерство транспорта и коммуникаций и Омбудсмен по защите данных (Data Protection Ombudsman).

Среди стран Центральной и Восточной Европы, которые получили членство в ЕС, ведущее место в разработке и внедрении политики информационной безопасности занимает Эстония. Разработкой и внедрением политики информационной безопасности занимается Министерство экономики и коммуникаций Эстонии, а точнее такие его структурные подразделения, как Департамент государственной информационной системы и Эстонский центр информатики [3].

В рамках ЕС информационная безопасность рассматривается как состояние информационных сетей и систем, обеспечивающих достаточный уровень защиты целостности, доступности и конфиденциальности информации, надлежащий уровень противодействия внешним негативным воздействиям. Одним из приоритетов политики стран ЕС в сфере информационной безопасности является разработка и внедрение программ и различных технических средств, которые позволяют поддерживать определенный уровень защиты информационно-коммуникационных технологий. Наряду с этим в рамках ЕС значительное внимание уделяется правовым основам информационной безопасности, предусматривающим разработку нормативно-правовых актов, которые устанавливали бы перечень преступлений, связанных с информационными технологиями, и определяли соответствующую уголовную ответственность. Другим приоритетом политики ЕС является информационная безопасность граждан. Фактически это высокий уровень

осведомленности общественности о рисках и угрозах, связанных с информационными технологиями, о способах защиты своих информационных систем/сетей от нежелательных воздействий. Сюда относятся не только противодействие кибератакам, но и защита персональных данных, обнаружение вредоносного контента в сети Интернет и тому подобное.

После провозглашения Украиной независимости начался процесс интеграции в мировые сообщества. Однако следует заметить, что внешняя информационная деятельность Украины в данном случае активизировалась недостаточно. В то же время в последние годы иностранная информационная активность относительно Украины увеличилась в десятки раз. Особенно сказывается влияние России. Информационный поток с Запада и Востока в Украине не имеет препятствий, а обратного – из Украины на Восток и Запад – фактически не существует.

Главными признаками, характеризующими информационную ситуацию в любой стране, являются такие: функционирование средств массовой информации (далее – СМИ) и пропаганды, функционирование информационно-аналитической системы, которая призвана обеспечивать эффективное принятие решений и контроль в сфере государственного управления, а также управления бизнесом. Все эти составляющие информационной ситуации в Украине следует характеризовать как негативные. В Украине отсутствует единая нормативно-правовая база. Доктрина информационной безопасности так и не была принята. Существует ряд государственных органов, которые дублируют свои функции в реализации информационной политики и обеспечении информационной безопасности.

Что касается информационно-аналитической деятельности в Украине, то она хоть и развивается, но этот процесс продолжается медленно и в основном экстенсивным путем (возникновение новых государственных и негосударственных информационно-аналитических структур и так далее). Это также может иметь негативные последствия, поскольку количество информации растет, а ее качество остается на низком уровне, недостаточном для принятия потребителями этой информации обоснованных решений. Состояние информационной деятельности Украины является неудовлетворительным, а отечественная информационная система функционирует на уровне стран «третьего мира», значительно отставая от развитых западных государств [4, с. 129].

Приоритетная задача в сфере обеспечения международной информационной безопасности связана с возможностью применения информационно-коммуникационных технологий (далее – ИКТ) в целях, не совместимых с задачами обеспечения международной стабильности и безопасности. Важнейшими угрозами считаем враждебное использование ИКТ на уровне государств против информационных инфраструктур в политических, в том числе военных, целях, преступную и террористическую деятельность в киберпространстве [5].

Одной из наиболее важных проблем продвижения в данном направлении является прежде всего достижение необходимого уровня политического доверия между правительствами государств мира. Известно, что это доверие возникает тогда, когда у основных субъектов международной политики имеются схожие взгляды на политическую ситуацию, на причины имеющихся дисгармоний и конфликтов в межгосударственных отношениях и путях снижения социально-политической опасности имеющихся разногласий.

В современном мире роль диалога в разрешении конфликтов увеличивается, хотя конфликтов не становится существенно меньше. Политические лидеры разных государств мира прилагают определенные усилия для укрепления доверия, однако значительную роль в решении этой проблемы играет гражданское общество, которое во многом определяет допустимый для страны уровень доверия в отношениях с тем или иным государством и, соответственно, диапазон возможных действий политических лидеров в этой сфере.

Для формирования системы обеспечения международной информационной безопасности считаем важным определить возможную цель международного соглашения в данной отрасли.

Такой целью могло бы стать создание механизмов международного сотрудничества в сфере обеспечения устойчивости функционирования и безопасности использования глобальной информационной инфраструктуры и ее национальных сегментов, безопасности информационных и телекоммуникационных технологий.

Под устойчивостью функционирования понимаем способность сохранять работоспособность в условиях воздействия определенных неблагоприятных факторов.

Под безопасностью понимается защищенность от угроз нарушения конфиденциальности и целостности информации, циркулирующей в глобальной информационной инфраструктуре и ее национальных сегментах, а также от угроз использования уязвимостей информационных и телекоммуникационных технологий для агрессивного нанесения ущерба международной и национальной безопасности государств-членов международного сообщества.

Достижение этой цели могло бы способствовать укреплению доверия к глобальной информационной инфраструктуре, информационным и телекоммуникационным технологиям как фактору устойчивого развития человечества.

Можно предложить следующие основные направления сотрудничества Украины в сфере формирования системы обеспечения международной информационной безопасности:

– поддержание устойчивости и безопасности функционирования глобальной информационной инфраструктуры и ее национальных сегментов, которое в определенной степени базируется на интернационализации управления пользованием и развитием глобальной сети Интернет;

– выявление опасных нарушений устойчивости и безопасности глобальной информационной инфраструктуры и ее национальных сегментов, информационных и телекоммуникационных технологий, связанное с налаживанием международного мониторинга этих процессов, юриди-

ческое закрепление выявляемых нарушений;

– проведение расследований по фактам опасных нарушений устойчивости функционирования и безопасности использования глобальной информационной инфраструктуры и ее национальных сегментов, безопасности информационных и телекоммуникационных технологий, связанное с выявлением уполномоченными международными органами лиц, действия которых привели к соответствующим нарушениям устойчивости и безопасности;

– разработка и принятие требований по устойчивости и безопасности глобальной информационной инфраструктуры и ее национальных сегментов, безопасности информационных и телекоммуникационных технологий, оценка выполнения данных требований;

– выработка и реализация предложений по повышению устойчивости и безопасности глобальной информационной инфраструктуры и ее национальных сегментов, безопасности информационных и телекоммуникационных технологий.

Первым шагом в этом направлении могла бы стать проработка международным экспертным сообществом вопросов относительно таких аспектов:

– терминологии, используемой в сфере обеспечения международной информационной безопасности;

– выработки общих подходов к определению объектов обеспечения международной информационной безопасности;

– проработки возможных механизмов международного сотрудничества в обеспечении безопасности данных объектов;

– проработки международно-правовых аспектов регулирования отношений в рассматриваемой сфере.

В процессе такой работы следует определиться с тем, на какой уровень сотрудничества в анализируемой сфере могут пойти государства-члены международного сообщества, а также применительно к этому уровню осуществить более детальную проработку научных, организационных, правовых, дипломатических и иных аспектов проблемы.

Основной целью политико-правового регулирования отношений в указанных направлениях сотрудничества могло бы стать формирование международных механизмов предотвращения или минимизации негативных последствий агрессивного использования информационных и телекоммуникационных технологий для разрешения межгосударственных противоречий.

Анализ проблем обеспечения информационной безопасности позволил сделать вывод, что наиболее важными направлениями деятельности в этой сфере являются всесторонняя оценка угроз и опасностей, национальной уязвимости, идентификация критической инфраструктуры. В процессе обеспечения информационной безопасности важно понимать характер, природу, сущность и содержание угроз и опасностей, уметь своевременно идентифицировать источник угрозы.

Выводы. Таким образом, совершенствование обеспечения информационной безопасности требует целенаправленного изучения зарубежного опыта организации и проведения информационных операций, методов, средств осуществления кибератак, а также моделирования информационных нападений. Дальнейшего решения требуют такие вопросы: разработки комплекса информационных стандартов обеспечения информационной безопасности, развития системы сертификации информационных продуктов, систем и услуг, создания системы лицензирования деятельности организаций по отдельным направлениям, формирования единого информационного пространства Украины.

Список использованной литературы:

1. Communication from the European Commission “Network and Information Security: Proposal for a European Policy Approach” : COM(2001)298 (June 6, 2001) [Электронный ресурс]. – Режим доступа : http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf.

2. The European Network and Information Security Agency (ENISA) [Электронный ресурс]. – Режим доступа : http://www.enisa.europa.eu.

3. ENISA Country Reports (2009) [Электронный ресурс]. – Режим доступа : http://www.epractice.eu/files/media/media2624.pdf.

4. Хімей В.В. Основні сучасні проблеми інформаційної безпеки України / В.В. Хімей // Телета радіожурналістика. – 2014. – № 13. – С. 127–132.

5. Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности / А.В. Крутских // Международные процессы [Электронный ресурс]. – Режим доступа : http://www.intertrends.ru/thirteen/003.htm.