

**Проблемы формирования нормативных основ международной
информационной безопасности**

Пащенко Илья Юрьевич

Студент (бакалавр)

Кубанский государственный университет, Краснодар, Россия

E-mail: ilpa001@mail.ru

Современные вызовы международной безопасности в информационной среде становятся все более очевидными. В эпоху глобализации и динамичного развития современных технологий возрастают угрозы в информационной среде. Проблемы обеспечения международной информационной безопасности затрагивают стратегические интересы всего мирового сообщества, и их решение возможно только путем взаимодействия всех участников международных отношений. Основная озабоченность в сфере обеспечения международной информационной безопасности (МИБ) связана с возможностью применения получивших беспрецедентное развитие информационно-коммуникационных технологий (ИКТ) и, в частности, глобальных сетей в целях, несовместимых с задачами обеспечения международной безопасности и стабильности [2]. На данный момент сформировалось лишь четкое представление о самих угрозах в информационной среде, но еще не создана сама система по обеспечению безопасности в информационной отрасли. В этой связи весьма актуален вопрос − возможно ли создание защищенной международной информационной системы?

Под информационной безопасностью можно понимать состояние защищенности основных интересов личности, общества и государства в информационном пространстве. Препятствие стратегическим интересам государств в области информационной безопасности может повлечь нарушение мировой стабильности и всеобщего правопорядка.

Определенный вклад в формирование правовых основ информационной безопасности внесен Советом Европы и СНГ. Члены Совета Европы приняли 23 ноября 2001 г. Конвенцию о киберпреступности. Положения Конвенции направлены на противодействие деяниям против конфиденциальности, целостности и доступности компьютерных систем, сетей и данных, а также неправомерного их использования, что достигается признанием этих деяний в качестве преступлений, а также применением соответствующих властных полномочий, направленных на обнаружение киберпреступлений, их расследование, судебное преследование лиц, их совершивших [7]. В рамках СНГ в 2001 г. было подписано Соглашение о сотрудничестве государств − участников СНГ в борьбе с преступлениями в сфере компьютерной информации. Однако, судя по статистике роста преступлений в данной сфере, организационные и правовые основы международного сотрудничества в борьбе с ними недостаточно эффективны.

На международной арене все чаще говорят о необходимости создания специального органа при ООН по обеспечению международной информационной безопасности. На данный момент на универсальном уровне отсутствует договор, комплексно регулирующий правоотношения в информационной сфере. Россия неоднократно на заседаниях Генеральной Ассамблеи ООН предлагала концепции и конкретные меры для обеспечения информационной безопасности. Важным достижением стало принятие 8 декабря 2010 г. Резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности» [5].

Особую позицию в вопросах формирования МИБ занимают Соединенные Штаты Америки, которые не поддерживают принятие международных актов в области информационной безопасности, игнорируя интересы мирового сообщества. США неоднократно на-

рушали принципы обеспечения информационной безопасности других стран. В феврале Kaspersky Labs Global Research and Analysis Team (GReAT) опубликовала отчет, в котором привела доказательства того, что хакерская команда «Equation Group» на протяжении нескольких лет работала совместно со спецслужбами США и внедряла вирус в программное обеспечение жестких дисков для получения всевозможных сведений [6]. Шпионы получали информацию из 42 стран мира, где огромное количество жёстких дисков компьютеров было изначально заражено вирусом. Россия одной из первых осознала опасности, связанные с милитаризацией информационного пространства и противоправной деятельностью в нем [1]. Российской Федерацией была предложена концепция Конвенции об обеспечении международной информационной безопасности, которая так и осталась проектом [4].

Формированию полноценной структуры по обеспечению МИБ могло бы послужить реальное снижение угрозы нарушения мирового правопорядка и обеспечение стабильности в информационном пространстве, недопущение враждебного воздействия на информационные системы отдельных стран, защита информации в целях полноценного развития государств. Применение информационного оружия в виду его специфики может повлечь нарушения систем информационной безопасности и копирования секретной информации, а это соизмеримо с использованием оружия массового уничтожения, так как может вывести из строя целые блоки государственных автоматизированных систем и комплексов.

Международная практика содержит целый ряд примеров враждебного воздействия на информационные системы [3]. Вредоносные технологии доступны не только ряду стран, но и группам лиц и различным неправительственным организациям, в том числе террористическим.

Представляется, что необходимо выработать международные стандарты для формирования единого подхода к обеспечению информационной безопасности, что откроет возможности, в том числе, и для полноценного обмена информацией между государствами в целях противодействия международной преступности. Важнейшие усилия в ближайшей перспективе в области МИБ следует направить на разработку необходимых правовых механизмов, повышающих доверие к глобальной информационной инфраструктуре, а также ограничить вмешательство государств в информационную среду региональных и внутригосударственных систем. Созданные правовые механизмы, в частности, по ограничению информационного влияния одних государств на другие, будут содействовать сохранению позитивного потенциала, который накоплен в настоящий момент в международном праве.

Источники и литература

- 1) Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. М., 2012. № 4 (13). С.119-136.
- 2) Шерстюк В.П. Угроза международной информационной безопасности в условиях формирования глобального информационного общества и направления сотрудничества // Право и безопасность. М., 2010 . № 4(37). С.24-27.
- 3) Шинкарецкая Г.Г. Враждебное воздействие на компьютерные системы государства и международное право // Российский ежегодник международного права, 2013. СПб., 2014. С. 236-238.
- 4) Конвенция об обеспечении международной информационной безопасности (концепция). URL:<http://www.scrf.gov.ru>. Дата обращения: 20.02.2015 г.
- 5) Резолюция Генеральной Ассамблеи Организации Объединенных Наций

A/RES/65/41 от 8 декабря 2010 г. URL: <http://www.un.org/ru>. Дата обращения: 15.02.2015 г.

- 6) Equation Group: The Crown Creator of Cyber-Espionage
URL:<http://www.kaspersky.com>. Дата обращения: 20.02.2015 г.
- 7) Европейская Конвенция по киберпреступлениям от 23.11.01 г.
URL:<http://www.base.garant.ru>. Дата обращения: 25.02.2015 г.