УКУК. САЯСАТ ТААНУУ
ПРАВО. ПОЛИТОЛОГИЯ
RIGHT. POLITICAL SCIENCE

Сманалиев К.М., Еримбетов С.С.

ЗАМАНБАП ЭТАПТАГЫ МААЛЫМАТТЫК КООПСУЗДУКТУН ГЛОБАЛДУУ КОРКУНУЧУ

Сманалиев К.М., Еримбетов С.С.

ГЛОБАЛЬНЫЙ ВЫЗОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СОВРЕМЕННОМ ЭТАПЕ

K.M. Smanaliev, S.S. Erimbetov

GLOBAL CHALLENGE TO INFORMATION SECURITY AT THE PRESENT STAGE

УДК:337/49.12

Макалада мамлекеттин укуктук мейкиндигинде маалыматтык коркунучтун пайда болуусу жана маалыматтык коопсуздукту камсыздо зарылчылыгы каралат.

Түйүндүү сөздөр: *маалыматтык коопсуздук, телекоммуникация, укуктук саясат, улуттук чек ара, эл аралык мейкиндик, компьютердик маалымат, коркунуч, кибернетика*.

The article discusses the importance of information security and emerging potential threats in the sphere of information security of the society and the state.

Keywords: information security, telecommunications, legal policy, national boundaries, international space, computer information, the threat cybernetics.

The article describes emerging information risk in the legal space of the state and the need to ensure information security.

Key words: *information security, telecommunications, legal policy, national border, international space, computer information, threat, cybernetics.*

Генеральная Ассамблея (ГА) ООН в своей резолюции отметила, что «достижения науки и техники могут иметь как гражданское, так и военное применение… [поэтому] призывает государства-члены содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных мер по ограничению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации» [1, с. 1, 3]. Причем это не первый документ, принятый ООН. Мировое сообщество пытается осмыслить все достижения и угрозы, которые таятся в технологическом рывке информационно-коммуникационных технологий (ИКТ). Впервые эта проблема была поднята в 1998 г. на заседании ГА ООН Российской Федерацией. Ежегодно Генеральный Секретарь представляет отчеты ГА, в которых находит отражение мнение членов ООН по данному вопросу.

Развитие ИКТ является весьма динамичной сферой мировой экономики, которая конкурирует с наиболее доходными ее отраслями (сельхоз продукция, топливно-энергетическая, автомобилестроение и др.). Поэтому информационная безопасность как существенная часть системы национальной, региональной и международной безопасности в условиях интенсивного развития информационной инфраструктуры нуждается в разработке целостного подхода в государственной политике, который не ущемляет конституционное право человека на информацию и обеспечивает безопасность общества и государства.

Поддержание международной безопасности была прямой целью создания ООН, она закреплена в Ст. 1 Устава ООН. На сегодняшний день информационная и телекоммуникационная безопасность переросли в разряд международных угроз современности в связи с зависимостью общества от устойчивости средств ИКТ, противоправной деятельности, разворачивающейся в этой области, как против личности, так и против государств и правительств. В предисловии к докладу второй Группы Правительственных Экспертов (ГПЭ) Генеральный Секретарь ООН Пан Ги Мун писал: «Генеральная Ассамблея призвана сыграть важную роль в процессе повышения безопасности информационных технологий и телекоммуникаций как на национальном, так и на международном уровнях» [2, с. 3].

Трансграничность информационного пространства привела к зависимости усилий по укреплению информационной безопасности национального государства от соответствующих действий других стран. Неравномерное развитие ИКТ и ее инфраструктуры в масштабах земного шара делают уязвимой глобальную сеть, создают благоприятную почву для новых угроз. Различия национальных законодательств и правовой практики существенно замедляют темпы формирования безопасной информационной среды, восстановления данных после несанкционированной информационной интервенции. Поэтому, по мнению

эксперта ГА, необходимо активизировать усилия в области передачи ИКТ развивающимся странам и помощь в наращивании «потенциала в вопросах профессиональной подготовки в вопросах безопасности» [2, с. 7].

Поддержание устойчивой международной информационной безопасности требует создания соответствующих условий безопасности компьютерных и информационных систем в сфере бизнеса, экономической деятельности, регулирования пространства Интернет. По признанию Группы правительственных экспертов (ГЭП) мотивация частных лиц и даже государств в нарушении запрете на доступ к конфиденциальной информации объяснима, поскольку информация, добытая преступным путем, может дать огромные выгоды. Повсеместность и широкая доступность ИКТ, которые являются ее специфическими свойствами, создают сложную конфигурацию взаимосвязанности телекоммуникационных, информационных и социальных сетей. Фактически любое устройство ИКТ может стать либо источником, либо объектом противоправных действий. Кроме того, их легко скрыть, для выявления противозаконных деяний требуется специальная подготовка в области информационных технологий. Лица, занимающиеся подобного рода деятельность, могут действовать безнаказанно практически в любой точке земного шара, поэтому ИКТ превращаются в идеальные средства подрывной деятельности. Например, по признанию экспертов кибер-преступность претерпевает очень сложный процесс, перерастая в хорошо организованную структуру, и выходит из национальных границ на международный простор. Ранее преступники действовали в одиночку или небольшими группами, получив персональную информацию о пользователях, ключи доступа к их картам и счетам, снимали деньги, что позволяло отследить, поймать и доказать их вину. Однако теперь «кибер-преступники специализируются на отдельных этапах преступления и действуют глобально, совершая преступления в других странах из регионов, где им сложнее будет предъявить обвинения» [3]. При этом криминальная инфраструктура (серверы, веб-страницы, электронные кошельки, банковские счета и т.д.) располагаются в-третьих странах, что усложняет их блокировку или уничтожение.

Трудности правового регулирования и обеспечения информационной безопасности в мире во многом исходят еще и из-за отсутствия общепринятых правовых норм в этой области. С целью устранения этого препятствия Пан Ги Мун указывает на то, что правительства государств-членов «только начали разрабатывать нормы, законы и формы сотрудничества, необходимые в этой новой информационной сфере» [2, с.3]. Для ускорения данного процесса экспертами предлагается «осуществление обмена информацией о национальных законах и национальных стратегиях обеспечения безопасности информационно-коммуникационных технологий и технологиях, принципах и передовых методах» [2, с.8].

Ни одно государство перед лицом столь глобальной проблемы не может эффективно бороться за национальную информационную безопасность в одиночку. Для этого требуются коллективные меры, которые во многом зависят от «выработки общей терминологии и определений в связи с положениями резолюции 64/25 Генеральной Ассамблеи» [2, с. 8].

Одной из серьезных проблем в информационной сфере несогласованность в употреблении правовых дефиниций. Унификация терминологического аппарата в области информационной безопасности сыграла бы важную роль «при формировании единого информационно-правового пространства» [4, с. 15]. Не менее сложной является проблема в борьбы с такими феноменами, как «информационный терроризм» и «информационная война».

Попытки террористов контролировать инфраструктуру ИКТ или использования их возможностей для проведения терактов уже имели место в истории XX-XXI вв. Но можно сделать предположение о том, что с дальнейшим углублением развития технологических инноваций такие попытки будут учащаться. К тому же государства-члены ООН проводят собственные исследования в области ИКТ в поиске дополнительных инструментов ведения войны и получения информации разведывательного характера, с последующим использованием в политических целях. Например, служащие Министерства обороны США предупреждают правительство о существовании ИКТ угроз национальной безопасности Америки. Поэтому Белый дом вынужден регулярно увеличивать ассигнования на создание технологий, способных противодействовать кибератакам. Пентагон одной из контрмер считает возможным осуществление прямой интервенции в компьютерные сети потенциальных стран-противниц США. Комплекс мер включает в себя: «перехват и введение ложной информации в сообщения, передаваемые по беспроводным каналам связи, рассылку фиктивных электронных писем, а также другие формы и методы нейтрализации враждебных действий по отношению к Соединенным Штатам в киберпространстве» [5].

Ни одно государство в мире в настоящее время не сумело разработать соответствующие статьи в своем законодательстве, которые адекватно и однозначно определяло бы преступления против информационной безопасности, а компьютерная информация являлось бы предметом преступного посягательства. ИКТ из разряда теоретической аналитики вопросов международных отношений вышло в плоскость практического применения в боевых условиях, что ставит остро проблему правового обеспечения информационной безопасности.

Литература:

1. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности // Резолюция Генеральной Ассамблеи ООН 2 декабря 2009 г.

A/RES/64/25.Доклад эксперта Генеральной ассамблеи. MIMUN 2014. 13-18 апреля 2014 г. 20 с. URL: http://modelun.ru/reports/GArep2014

2. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности / Управление по вопросам разоружения. ООН. – Нью-Йорк, 2012.– 66 с. URL: http://www.un.org/ disarmament/ HomePage/ ODA Publications/DisarmamentStudySeries/PDF/DSS33_Russian
3. Короткин А. Кибер-преступность стала серьезной угрозой в России и в мире //Digital газета. 3 декабря 2014г. URL: http://digital.gazeta.ru/articles/kiber-prestupnost_tala_sereznoi_ugrozoi_v_rossii_i_v_mire.shtml
4. Химченко А.И. Информационное общество: правовые проблемы в условиях глобализации : автореф. дис. … к.ю.н. 12.00.13 / А.И. Химченко. – М., 2014. – 23 с.
5. Иванов В. Пентагон создает кибервойска / В. Иванов // Независимое военное обозрение. 11 декабря 2009. URL: http://nvo.ng.ru/forces/2009-12-11/14_ kibervoiska. html

Рецензент: д.полит.н., профессор Артыкбаев М.