



СМИ под защиту

Наталья ДОВНАР,
доцент факультета журналистики БГУ:

– Стратегия развития информационного общества в Республике Беларусь на период до 2015 года, утвержденная Постановлением Совета Министров Республики Беларусь от 09.08.2010 четко обозначила доминирующую роль знаний и информации во всех сферах человеческой деятельности и общества в целом. Государственная информационная политика, в этой связи, охватывает всю совокупность общественных отношений, связанных с созданием, накоплением, хранением, обработкой и распространением всех видов информации, в числе которых определенное место занимают средства массовой информации (СМИ). Решение задач обеспечения информационной безопасности в сфере СМИ осуществляется на основе реализации комплекса взаимосвязанных политических, экономических, правовых мер, направленных на выявление, предупреждение и нейтрализацию различных вызовов и угроз безопасности личности, общества и государства. В части правового обеспечения действует целый ряд международных соглашений, нормативных правовых актов Республики Беларусь, специальное законодательство (Закон Республики Беларусь «О средствах массовой информации»), которые позволяют в большинстве случаев нейтрализовать угрозы национальным интересам. Однако сегодня можно констатировать: стремительное развитие информационных технологий намного опережает развитие правовых механизмов регулирования общественных отношений в информационной сфере с учетом новых жизненных реалий. Это стало особо проявляться, когда четко обозначились структурные изменения в СМИ и всей медиаиндустрии, связанные с техническими новинками, прежде всего переводом содержания (текста, графики, звука) в цифровую форму. Цифровизация содержания привела к тому, что «Интернет из сети, технически соединяющий множество компьютеров, превратился в особую инфокоммуникаци-

онную среду, где цифровое содержание «старых» СМИ дополняется контент-продуктами и услугами, предоставляемыми только новыми медиа.

Интернет-СМИ рассматривается сегодня не только как источник информации, но и как площадка для дискуссий, диалога, проявления гражданских инициатив. Это положительный момент коммуникационно–информационной деятельности СМИ. Однако субъекты коммуникации, оказавшись на этой площадке, по-разному понимают ее роль. Двусторонний обмен информацией чаще всего происходит в Интернет – СМИ между профессиональным журналистом и пользователем (пользователями). Журналист, при этом, высказывая свое мнение, давая оценки, как правило, осознает свой статус, а соответственно, права и обязанности, возложенные на него законом, правилами этики. Если он забудет эти правила – будет отвечать перед законом не только он, но и средство массовой информации, которое он представляет. Пользователями, чаще всего не чувствуют этой ответственности. «Интернет – помойка, а блогер – не человек, а субстанция, который говорит, что хочет. Лучше не показывать свое лицо, тогда никто не видит и никакой ответственности», – считает один из активистов-пользователей. Такая позиция приводит порой к нарушению прав других лиц (чести и достоинства, частной жизни), распространению недостоверной информации.

В сложившейся ситуации представляется необходимым разработать Концепцию информационной безопасности в сфере массовой информации, в которой будут определены цели, задачи, направления деятельности субъектов информационной сферы, разведены понятия «средства массовой информации» и «средства массовой коммуникации», что позволит определить адекватные механизмы отношений, как в той, так и другой сфере.

Необходима систематизация

Ольга ЧУПРИС, старший научный сотрудник
Института правовых исследований Национального центра законодательства и правовых исследований Республики Беларусь:

– Современные информационные технологии не только открывают безграничные возможности, но и порождают проблемы (опасности, угрозы, вызовы). Информационное пространство по сути становится глобальным, единым. Соответственно этому требуется и объединение усилий государств в этой сфере не только с точки зрения организационных механизмов, но и правового регулирования, которое выступает важным обеспечительным средством этой безопасности.

Правовое регулирование в сфере безопасности информационного пространства Союзного государства и государств-участников в настоящее время находится в стадии накопления правового массива. Однако основной акт Союзного государства о безопасности Союза Беларуси и России и ее составляющей – информационной безопасности – Концепция безопасности этого Союза не изменялся с 1999 года. Вместе с тем, Концепция должна содержать актуальные направления обеспечения безопасности, в соответствии с которыми следует корректировать национальное законодательство и правоприменительную деятельность. Особенно это относится к такой мобильной сфере как информационная сфера, применительно к которой следует отметить необходимость пересмотра положений Концепции каждые 3-4 года. Это позволит также обеспечить предупреждение возможных негативных последствий опасности в информационной сфере.

Правовое обеспечение информационной безопасности в Союзном государстве и государствах-участниках в настоящее время строится с учетом выработки как общих принципов и направлений этой безопасности, так и установления специальных правовых режимов для отдельных сфер, к которым относятся военная безопасность, безопасность средств массовой инфор-

мации и др. Специальные правовые режимы предусматриваются для информации закрытого и ограниченного доступа (персональные данные, государственная, служебная тайна и т.п.), правовой информации. Эти режимы, охватывающие как критические инфраструктуры, так и инфраструктуры совместного ведения, получают закрепление в специальных нормативных правовых актах, регламентирующих то или иное направление деятельности в государстве. Следует рассмотреть возможность для определения в ближайшей перспективе правового Интернет-режима для обеспечения его безопасности. Вместе с тем, очевидно, что глобальный характер Интернета значительно ограничивает возможности отдельных государств в сфере регламентации порядка его использования.

Правовое регулирование в сфере информационной безопасности не может осуществляться вне его связи со всей системой законодательства. Системность и взаимосвязанность правовых норм позволяет «задействовать» эту систему в целом. Поэтому установление прав и обязанностей отдельных субъектов информационного пространства возможно в пределах нормативных правовых актов, прямо не относящихся к информационному законодательству. В частности, требования к воспитанию информационной пользовательской культуры могут быть сформулированы в законодательстве о браке и семье и об образовании, а соответствующие требования к кадрам – в законодательстве об образовании и государственной службе.

В качестве отдаленных перспектив развития законодательства в сфере безопасности информационного пространства Союза Беларуси и России следует рассматривать возможности систематизации этого законодательства.

Безопасность информационного

С 17 по 20 мая в Гродно прошла 16-я Научно-практическая конференция

Комплексный подход

В обеспечении национальной безопасности государств неуклонно возрастает роль защиты информации. Об этом заявил заместитель начальника Оперативно-аналитического центра при Президенте Беларуси – начальник управления защиты информации Сергей Капариха.

По его словам, универсальный подход к анализу задач повышает авторитет вышеупомянутой конференции, которая проводится под эгидой Союзного государства России и Беларуси уже в шестнадцатый раз.

«Конференция проходит на фоне стремительных процессов внедрения информационно-ком-



Сергей Капариха

муникационных технологий во все сферы жизнедеятельности в Беларуси и России. Однако наряду с достижениями в этой области мы сталкиваемся с новыми угрозами национальной безопасности», – отметил Сергей Капариха. В последнее время все чаще фиксируются факты компьютерных инцидентов в информационных системах Беларуси и других стран. В течение 2009-2011 годов в Беларуси неоднократно фиксировались сбои в функционировании системы обработки безналичных расчетов банковских пластиковых карточек Банковского процессингового центра.

В конце 2010 года и апреле 2011 года зафиксированы многочисленные DDoS-атаки на сайты государственных органов республики. Причем атакам подвергаются не только госресурсы, но и социальные сети и коммерческие сайты. Сейчас, в частности, широко обсуждается факт хищения из мультимедийных сетей компании Sony личных данных 77 млн человек, имеющих там персональные счета. Эксперты зафиксировали вторжение 27 апреля этого года, хотя, по их же мнению, хакерская атака состоялась еще 20 апреля.

В прошлом месяце текущего года в Москве был задержан злоумышленник, который путем дистанционного доступа к компьютеру бухгалтера одной из фирм получил контроль над счетами этой фирмы и похитил 5 млн российских рублей.

Атакам подвергаются и сети беспроводного доступа. Например, сейчас в США, в Сиглте полиция расследует ряд преступлений, в результате которых путем несанкционированного подключения к Wi-Fi сетям похищено более \$750 тыс.

Как отметил Сергей Капариха, одним из наиболее важных направлений является защита государственных секретов, в связи с чем на законодательном уровне приняты соответствующие меры.

Докладчик также подчеркнул, что важнейшим фактором успеха в области развития информационных технологий является наличие высококвалифицированных кадров, способных создавать современные программы и программно-технические решения и обеспечивать их безопасность. В Беларуси развивается вузовская система подготовки и повышения квалификации кадров в сфере информационной безопасности. В течение двух последних лет организована подготовка по специальности «компьютерная безопасность» в Гродненском и Полоцком государственных университетах. Специалистов в области защиты информации до этого готовили только столичные вузы: БГУ, БГУИР и БНТУ.

Несмотря на определенные успехи в образовательной политике, проблема нехватки высококвалифицированных специалистов остается весьма острой. Поэтому в дальнейшем государство будет уделять пристальное внимание вопросам образования в сфере безопасности информационных технологий, сообщил Сергей Капариха.



Игорь Войтов

программных средств и организационных мероприятий на всех этапах разработки, испытаний и эксплуатации информационных систем. Требования по защите, предъявляемые к информационной системе, должны рассматриваться как часть общих функциональных требований к ней.

Научно-техническое обеспечение развития информатизации в республике в рамках программы «Электронная Беларусь» в 2006-2010 годах и подготовки Стратегии развития информационного общества в Республике Беларусь на период до 2015 года (утверждена Постановлением Совета министров Республики Беларусь от 09.08.2010 №1174) осуществлялись на основе Государственной комплексной целевой научно-технической программы «Информационные технологии» (государственный заказчик – НАН Беларуси).

Данная программа была на-

формации», взаимодополняющих друг друга в рамках приоритетного направления научной и научно-технической деятельности «Информационные и телекоммуникационные технологии».

Новые угрозы

Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН) Михаил Вус напомнил, что концептуальным проблемам информационной безопасности в Союзе России и Беларуси была посвящена научно-практическая конференция, проведенная в Санкт-Петербурге в 2000 году. На конференции поднимались вопросы гармонизации законодательства в рамках Союзного государства, отмечалась необходимость организации проведения совместных исследований учеными и специалистами двух суверенных государств, в частности исследований по унификации правовых тезаурусов и классификаторов.

В итоговом документе конференции отмечалось, что «информационное пространство России и Беларуси требует единых подходов в защите от внешней информационной агрессии», в связи с этим подчеркивалась необходимость разработки Конвенции информационной безопасности для Союза Беларуси и России. В рекомендациях конференции обращалось внимание на необходимость «обеспечить включение в индикаторы оценки состояния информационной безопасности угрозы мировоззренческим факторам формирования

распространению информационного оружия на уровень глобальной проблемы безопасности. За прошедшие десятилетия проблемы информационной безопасности неизмеримо обострились. Угрозы информационно-технологического характера стали сегодня серьезным вызовом международной безопасности. На сегодня в мире уже фактически сложился новый вид организованной преступности, специализирующийся на преодолении (взломе) защиты компьютерных систем, хищении секретов и денежных средств, а известные события сентября 2001 года стерли грань между криминальной и военно-политической составляющей обеспечения международной информационной безопасности.

Всемирная федерация ученых поставила угрозу международной информационной безопасности на первое место в списке угроз человечеству в XXI веке. Объективно возникла потребность в международно-правовом регулировании мировых процессов гражданской и военной информатизации. Назрел вопрос разработки на международном уровне нормативно-правовых актов, регулирующих трансграничный информационный обмен, обеспечивающих защиту национальных информационных ресурсов, минимизирующих негативное информационное воздействие на массовое сознание, запрещающих использование информационно-кибернетических технологий в враждебных (деструктивных, агрессивных) целях против согласованных категорий объектов (критических объектов и технологий). В связи с этим следует отметить, что в Окинавской Хартии глобального информационного общества, подписанной в 2000 году «восьмеркой» ведущих государств, закреплены лишь вопросы целостности информационных сетей и пресечения преступлений в компьютерной сфере и фактически проигнорирована военно-политическая составляющая проблемы международной информационной безопасности.

Российская Федерация и Республика Беларусь являются членами Организации Объединенных Наций, в рамках которой на протяжении последнего десятилетия иницируются процессы поиска путей укрепления международной информационной безопасности. В рамках ООН неоднократно было озвучено предложение России (при поддержке Беларуси, Бразилии, Китая и ряда других стран) о необходимости исследования военно-политической составляющей угрозы международной информационной безопасности. Единственной страной, голосовавшей против, оказались США. Национальная политика США ориентирована на объединение (связывание) мирового сообщества глобальным кибернетическим пространством, которое – в силу технологического лидерства – подконтрольно американскому правительству и регулируется международно-правовыми нормами, не предусматривающими не только никакой ответственности за проведение политически мотивированных кибернетических атак, но даже не упоминания об их существовании в принципе. Стремясь вычленил из общего контекста проблемы обеспечения международной информационной безопасности вопросы исключительно киберпреступности и кибертерроризма, США выступают не только против выработки юридически обязывающих документов в области международной информационной безопасности, но даже «отказываются от работы по формированию терминологического глоссария по проблематике международной информационной безопасности в любой ее форме».

Международное сотрудничество апологетам информационных войн видится «преимущественно в форме распространения западного опыта, методик и технических средств по обеспечению защиты информационных и телекоммуникационных систем и сетей, что, в свою очередь, может представлять им возможность обеспечивать для себя прозрачность и контроль информационного пространства других государств и содействовать своей



применения систем обработки и распространения информации наблюдается рост количества случаев несанкционированного использования, модификации и уничтожения информации. Угрозы вычислительному и информационному ресурсам не могут быть выявлены, локализованы и ликвидированы внедрением в информационные системы отдельных аппаратных, программных средств и организационных мероприятий. Все средства и мероприятия должны быть объединены в систему защиты. Защиту информации следует рассматривать как регулярный процесс, осуществляемый путем комплексного использования технических,

правлена на создание новых интеллектуальных информационных технологий и систем, разработку моделей, математических методов и программно-аппаратных средств для повышения конкурентоспособности продукции и развития социальной сферы страны. Государственная комплексная целевая научно-техническая программа «Информационные технологии» представляла собой комплекс из государственной комплексной программы научных исследований «Научные основы информационных технологий и систем (Инфотех)» и двух государственных научно-технических программ «Информационные технологии» и «Защита ин-

личности и жизнеберегающим ресурсам развития общества».

Сказанное не потеряло своей актуальности и сегодня. Угрозы использования информационно-коммуникационных технологий в преступных, террористических и военно-политических целях, несовместимых с обеспечением международной безопасности, могут реализовываться как в гражданской, так и в военной сферах и привести к тяжелым политическим и социально-экономическим последствиям в отдельных странах, регионах и в мире в целом, к дестабилизации общественной жизни государств. Все это вывело задачи защиты информации и противодействия