УДК 342 (004.056.53)

СОЗДАНИЕ НОВЫХ МЕХАНИЗМОВ СИСТЕМНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

CREATION OF NEW MEASURES FOR THE PROTECTION OF INFORMATION SYSTEM IN THE REPUBLIC OF BELARUS

А.А.Григорьев, научный сотрудник НИИ теории и практики государственного управления, Академия управления при Президенте Республики Беларусь
А.А.Охрименко, декан факультета компьютерных технологий, Институт информационных технологий, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент
И.П.Сидорчук, заместитель директора НИИ теории и практики государственного управления, Академия управления при Президенте Республики Беларусь, кандидат юридических наук, доцент

A.A. Grigoriev, Researcher of the Institute of Theory and Practice of Public Administration, Academy of Public Administration under the aegis of the President of the Republic of Belarus
A.A.Ohrimenko, Dean of Faculty of Computer Technologies, Institute of Information Technologies, Educational Establishment «Belarusian State University of Informatics and Radioelectronics», Ph.D., associate professor
I.P.Sidorchuk, Deputy director of the Institute of Theory and Practice of Public Administration , Academy of Public Administration under the aegis of the President of the Republic of Belarus, PhD, associate Professor

Адрес электронной почты: ohrimenko@bsuir.by

Аннотация. В статье рассматриваются правовые основы состояния и развития национальной информационно-коммуникационной инфраструктуры, интегрированной в систему государственного управления Беларуси. В рамках комплексного анализа проблемных вопросов обеспечения безопасности государственных информационных систем и нормативного правового регулирования в этой сфере обосновываются предложения, направленные на минимизацию угроз при использовании средств электронных коммуникаций в условиях электронного правительства.

Annotation. The article deals with the legal framework conditions and development of national information and communication infrastructure, integrated into the system of government of Belarus. As part of a comprehensive analysis of problematic issues of security of government information systems and normative legal regulation in this area justified proposals aimed at minimizing the threats of using means of electronic communication under the e-government.

Ключевые слова: информационно-коммуникационные технологии, средства электронных коммуникаций, нормативные правовые акты, взаимное сотрудничество государств, минимизация угроз обществу и государствам, международное сообщество.

Key words: information and communication technologies, electronic communication, regulations, mutual cooperation of the states, minimizing threats to society and the state, the international community.

Процессы глобализации, транснациональные вызовы, политические конфликты выдвигают новые требования к государственному строительству и государственному управлению, эффективность которых на современном этапе неразрывно связана с совершенствованием и активным применением средств информационно-коммуникационных технологий (далее – ИКТ). Использование ИКТ для модернизации системы государственного управления, внедрение инновационных IT-проектов, создание электронного правительства, переход на электронный документооборот в органах власти, реализация государственных услуг в электронном виде позволяют существенно экономить бюджетные средства, увеличить скорость принятия управленческих решений, а также способствуют борьбе с коррупцией.

Республика Беларусь продвинулась в развитии электронного правительства и электронных услуг. Темпы развития ИКТ в области государственного управления в Беларуси отмечают международные эксперты. Данные статистического сборника ООН «Электронное правительство. Обзор 2014» свидетельствуют, что Беларусь улучшила свои позиции и занимает 55 место из 193 стран мира [1].

В результате выполнения государственных, отраслевых и региональных программ разработан ряд общегосударственных и ведомственных информационных систем, создана национальная система формирования и регистрации информационных ресурсов. Республиканские органы государственного управления, облисполкомы, Мингорисполком, а также иные исполнительные и распорядительные органы представлены в сети Интернет.

В стране создается единая республиканская сеть передачи данных (далее – ЕРСПД), являющаяся мультисервисной сетью электросвязи, и объединяющая сети передачи данных государственных органов и иных государственных организаций, юридических лиц негосударственной формы собственности и индивидуальных предпринимателей в добровольном порядке. Введена в эксплуатацию опорная сеть для ЕРСПД.

В рамках формирования в Беларуси электронного правительства информационные системы и ресурсы отдельных государственных органов и иных государственных организаций интегрируются в единое информационное пространство, основными элементами которого определены:

система межведомственного информационного взаимодействия государственных органов и иных государственных организаций;

государственная система управления открытыми ключами;

государственная система оказания электронных услуг.

Возможность мобильной передачи данных в больших объемах, их ускоренная обработка, возможность упрощенного хранения и быстрота доступа к ним сделали привлекательным использование ИКТ и их интеграцию в

систему государственного управления, в том числе при работе с обращениями граждан и юридических лиц.

В соответствии с новой редакцией Директивы Президента Республики Беларусь от 27 декабря 2006 года № 2 «О дебюрократизации государственного аппарата и повышении качества обеспечения жизнедеятельности населения» определен ряд приоритетов для деятельности государственных органов Республики Беларусь в сфере ИКТ [2]. Их сутью является полномасштабный переход государственных органов к электронному документообороту при реализации государственных функций, в том числе рассмотрении обращений граждан и юридических лиц, осуществлении административных процедур.

В целях реализации названного документа широко внедряются в практику государственных структур как предварительная запись на личный прием с помощью электронных средств связи, так средства электронного управления очередью. Кроме того, разработан проект Стратегии развития информатизации на 2016−2022 гг., предусматривающий план конкретных мероприятий в различных областях - социальной сфере, реальном секторе, транспортной отрасли, банковском секторе [3]. Например, в ходе реализации Стратегии запланирован полный перевод медицинской документации в электронный вид. Кроме того, Стратегия должна способствовать оптимизации взаимодействия государства и населения. В частности предполагается, что доля услуг, оказываемых государственными органами в электронном виде, должна составлять не менее 75%. В целом электронный документооборот в госорганах должен составить не менее 95%.

В рамках Директивы Президента Республики Беларусь от 27 декабря 2006 года № 2 Совету Министров Республики Беларусь совместно с облисполкомами и Минским горисполкомом поручено на постоянной основе обеспечивать актуализацию сведений, содержащихся на интернет-сайтах государственных организаций и подчиненных им организаций, в целях исключения противоречивой, неактуальной информации, восполнения пробелов в информировании населения.

В дополнение к данным мерам руководителям государственных организаций предписано расширить практику общественного обсуждения на интернет-сайтах этих организаций наиболее значимых проектов нормативных правовых актов, обеспечивая путем использования результатов такого обсуждения вовлечение граждан в управление государством и, создавая надежный барьер коррупции.

Отмеченные подходы способствуют повышению доступности системы государственного управления и приближению её непосредственно к населению, что является наиболее важным при демократизации общества и установлению взаимной обратной связи государственных структур и общества.

В условиях построения открытого информационного общества тема защиты информационных ресурсов является особенно значимой для государственных органов, граждан и организаций в контексте роста преступлений с использованием ИКТ или киберпреступлений. Киберпреступность рассматривается как стремительно нарастающая угроза

безопасности национальным интересам отдельных государств, так и для мирового сообщества в целом. Результаты опросов, изучение материалов судебных слушаний, наблюдения ученых позволяют утверждать, что мировое сообщество столкнулось с серьезными проблемами в этой сфере. В развитых странах уровень киберпреступности измеряется тысячами правонарушений, а экономический ущерб составляет миллиарды долларов США.

Поэтому нормальное функционирование электронного правительства зависит от надежности средств коммуникации, электросвязи, программных продуктов, хранилищ информации и обеспечивающих их средств. Все это предъявляет особые требования к вопросам безопасности сетевых ресурсов государственных органов, бесперебойности предоставления сервисов и соблюдения законодательных требований.

Использование ИКТ в системе государственного управления делает ее более уязвимой, в том числе при осуществлении актов киберпреступности, несанкционированного доступа к государственным информационным и финансовым системам, террористических актов и ведении боевых действий, иной антигосударственной и антиобщественной деятельности. Это создает ряд угроз, проблемные аспекты которых, недостаточно полно нашли свое отражение в праве Республики Беларусь.

Существующее законодательство большинства стран также пока еще недостаточно развито и адаптировано к противодействию таким угрозам и традиционно отстает от развития современных ИКТ. Это позволяет различным организованным противоправным группам похищать и продавать конфиденциальную информацию, персональные данные, денежные и кредитные средства, осуществлять несанкционированные действия против национального сегмента сети Интернет.

В данных условиях особую важность приобретает надежное и бесперебойное функционирование государственных электронных систем в условиях информационного противоборства, применения оружия массового поражения, иных видов оружия, защиты от террористических атак, массовых беспорядков, стихийных бедствий, недопустимость несанкционированного изменения данных. При этом особую важность в демократическом обществе представляет исключение возможности причинения вреда гражданам и организациям (государству), которые становятся существенно уязвимыми при недостатках защиты применяемых технических систем.

Представляется, что в данных условиях государственные органы должны использовать только программное обеспечение, оборудование, каналы связи (иную инфраструктуру), исключающие возможность хранения и передачи информации с использованием облачных технологий за рубежом без согласия Республики Беларусь в лице уполномоченных государственных структур. Предлагается определить порядок использования систем, предоставляющих информацию о персональных данных иностранным государствам (их государственным и иным организациям) с учетом согласия Республики Беларусь и лиц, данные о которых передаются. Обладатели информации или операторы информационных систем обязаны предотвращать

несанкционированный доступ к распространяемой ими информации. Вместе с тем данные меры не являются исчерпывающими, предлагается применять комплексный подход на основе мероприятий правового, идеологического и технико-технологического и иного характера, исходя из имеющегося набора угроз.

Существующие риски можно условно классифицировать на угрозы, представляющие опасность международному сообществу, государству, обществу в целом, включая негосударственные структуры, а также угрозы отдельным личностям. Учитывая их степень опасности необходимо предпринимать меры защиты как на межгосударственном, так и на национальном уровне в приоритетном порядке в рамках правовой регламентации общественных отношений. Актуально также формировать единую гражданскую позицию, способствующую неприемлемости сохранения в обществе соответствующих противоправных действий.

В данной сфере, по нашему мнению, заслуживает уважения опыт такой международной организации, как Совет Европы, в которой еще 28.01.1981 была подписана Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) [4]. Содержание норм данной Конвенции, закреплённых в статье 7, о защите персональных данных, хранящихся в автоматизированных файлах, данных, направленных на предотвращение их случайного или несанкционированного уничтожения, или случайной потери, а также на предотвращение несанкционированного доступа, их изменения или распространения таких данных, имеет четкую практическую направленность. Однако имеются факты, свидетельствующие о неспособности государственных структур ряда стран обеспечивать защиту персональных данных даже руководителей государств, результатом чего явилась недавняя утечка, очевидно, по техническим причинам, персональных данных В. Путина, Б. Обамы и А. Меркель, имевшихся у властей Австралии. Следует отметить, что данная Конвенция носит региональный характер (Австралия в ней не участвует).

При этом не все государства региона, даже имеющие тесные интеграционные связи, в том числе при электронном обмене персональными данными, при регламентации визовых вопросов в Союзном государстве, участвуют в ней. Например, Беларусь не участвует в данной Конвенции, которая действует для всех сопредельных с ней государств: Латвии – с 01.09.2001, Литвы – с 01.10.2001, Польши – с 1.09.2002, России – с 01.09.2013, Украины – с 01.01.2011. Для усиления международно-правовой защиты в данной сфере представляется целесообразным присоединение Беларуси к данной Конвенции, а также разработка и принятие универсального международного договора в рамках ООН. Для стран постсоветского пространства также актуально принятие договоров в рамках СНГ, Евразийского Экономического Союза, Союзного государства с учетом специфики соответствующих интеграционных структур, которые не могут избежать процессов связанных с защитой персональных данных граждан соответствующих государств.

Остается нерешенным вопрос о правовой защите граждан и организаций при деятельности глобальных поставщиков услуг, в том числе безвозмездных в данной сфере, которые используют персональные данные, предоставляют услуги электронных «почтовых» серверов, поисковых систем и т.п. Например, вызывает сомнение правомерность прекращение компанией Google обслуживания жителей Крыма под предлогом санкций и в связи с их переходом под юрисдикцию России. В данном контексте, не ясно, если данную территорию Google признает территорией Украины, то почему санкции применяются в отношении её граждан, которые остаются на ней проживать. Если данные меры принимаются против граждан Украины, массово перешедших в гражданство России, то не ясно, почему производится выборочная дискриминация граждан России по признаку их территориального проживания. Представляется, что дальнейшее развитие социальных сетей и сервисов, требует международно-правовой регламентации их деятельности в целях исключения нарушения прав государств, организаций и граждан.

В пункте 42 Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, в числе внешних источников угроз национальной безопасности в информационной сфере названы среди прочих: открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия; доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами; нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве; попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам [5].

При этом широкое распространение получили попытки внедрения криминальных структур в информационное пространство, в том числе в целях распространения наркотиков, вербовки наемников, внедрения в общественное сознание противоречащих общечеловеческим и национальным духовно-нравственным ценностям взглядов, что требует безотлагательной реакции как Республики Беларусь, так и иностранных государств, в рамках обеспечения международного сотрудничества. Не случайно, уровень угроз повлек к объединению усилий для устранения противоправной деятельности даже государств с различными политическими системами и доминирующими моральными ценностями, таких как США и КНР.

Республика Беларусь также не остается в стороне от данных процессов примером чему служит ряд новых нормативных правовых актов в данной сфере, в том числе Декрет Президента Республики Беларусь от 28 декабря 2014 г. № 6 «О неотложных мерах по противодействию незаконному обороту наркотиков» [6], постановление Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 г. № 6/8 «Об утверждении Положения

о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет» [7]. Данные документы позволили безотлагательно отреагировать на ряд общественно опасных угроз, в том числе, связанных с распространением опасных психотропных веществ.

Несмотря на принятие ряда мер, направленных на защиту общества от неблагоприятных процессов в глобальной компьютерной сети Интернет, а также направленных на повышение доступности государственной власти и активизацию ее присутствия в данной сети, например, Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» [8], ряд вопросов остается недостаточно урегулированным. Например, четко не определен правовой статус договоров об обмене информацией о персональных данных граждан и юридических лиц (относятся ли данные договоры к сфере административного или гражданского права, каков характер ответственности за их нарушения, как решать вопросы в части понуждения к заключению договора, возмещению убытков и т.п.), что существенно препятствует правовой защите прав и свобод граждан, и организаций, затрудняет реализацию их обязанностей.

В этой связи полагаем, что указанные вопросы должны найти свое нормативное отражение в виде специальных правил. Целесообразно также рассмотрение вопроса о централизации данных процессов и устранении необходимости многоступенчатой системы передачи данных, например, при принятии решений об ограничении доступа к информационным ресурсам. В ряде государств такие функции сконцентрированы у специализированных правоохранительных структур, что исключает вовлечение в данный процесс различных организаций, не относящихся к системе органов обеспечения национальной безопасности. При этом зачастую различными государствами ставится вопрос о законности такой деятельности [9].

При этом сохраняет важность вопрос уязвимости государственных информационных систем при монополизации отдельных программных продуктов и технологических систем зарубежными коммерческими организациями, которые в ряде случаев осуществляют широкомасштабное сотрудничество с правоохранительными и разведывательными структурами иностранных государств. Представляется, что решению данных проблем могло бы способствовать формирование независимого программного продукта и технических средств индивидуально ориентированных на государственные нужды с учетом специфики функционирования государственных структур.

В связи с глобализацией отношений, усилением миграции, требует универсального правового решения проблемы рассмотрения электронных обращений граждан и организаций, осуществления в отношении их административных процедур, которые не во всех случаях могут идентифицироваться при помощи электронной цифровой подписи (при этом данный вид идентификации также не является абсолютно надежным при появлении копий таких ключей). Данный вопрос может быть урегулирован

нормами международных договоров. При этом в таких договорах следует особо оговорить правила, исключающие ответственность чиновников и иных лиц, рассматривающих обращения, при рассмотрении сообщений, сформированных виртуальными машинами, в том числе с использованием вымышленных или похищенных персональных данных, учитывая, что соответствующие права, свободы и обязанности при формировании электронных обращений могут существовать только у реальных граждан и организаций, а не у виртуальных или иных механизмов и структур.

Основными способами противодействия указанным угрозам следует признать их своевременную профилактику и предупреждение, разработку эффективного законодательства, принятие взаимоувязанных национальных и международных нормативных правовых актов, учитывающих тенденции развития компьютерных преступлений.

Необходимо также уделять особое внимание развитию системы непрерывного повышения квалификации государственных служащих, их самообразования, рациональному управлению их знаниями, навыками и умениями в области ИКТ, а также постоянному росту профессиональной компетенции сотрудников правоохранительных органов, занимающихся раскрытием, расследованием и пресечением преступлений в сфере ИКТ.

Таким образом, представляется оправданным усиление взаимного сотрудничества государств, в том числе в лице чиновников и научных работников различных областей знания, в целях минимизации угроз обществу и государствам, международному сообществу в целом при использовании средств электронных коммуникаций.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. United nations e-government survey 2014 // [Электронный ресурс]. – 2015. – Режим доступа: http:// unpan3.un.org/egovkb/portals/egovkb/documents/un/2014-survey/e-gov_complete_survey-2014.pdf. – Дата доступа: 11.11.2015.

2. О дебюрократизации государственного аппарата и повышении качества обеспечения жизнедеятельности населения: Директива Президента Респ. Беларусь, 27 дек. 2006 г., № 2: в ред. от 23.03.2015 // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2015.

3. Проект стратегии развития информатизации в Беларуси на 2016-2020 годы вынесут на общественное обсуждение // [Электронный ресурс]. – 2015. – Режим доступа: http://www.belta.by/society/view/proekt-strategii-razvitija-informatizatsii-v-belarusi-na-2016-2020-gody-vynesut-na-obschestvennoe-3646-2015. – Дата доступа: 11.11. 2015.

4. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера (ETS N 108). Заключена в г. Страсбурге 28.01.1981 г., (с изм. от 08.11.2001) // [Электронный ресурс]. – 2015. –

Режим доступа: http://conventions.coe.int/ Treaty/RUS/Treaties/html/108.htm. – Дата доступа: 11.11.2015.

5. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Республики Беларусь, 9 нояб. 2010 г. № 575: в ред. Указа Президента Республики Беларусь от 24.01.2014 г. № 49 // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2015.

6. О неотложных мерах по противодействию незаконному обороту наркотиков: Декрет Президента Респ. Беларусь, 28 дек. 2014 г., № 6 // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2015.

7. Об утверждении Положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет: постановление Оперативно-аналитического центра при Президенте Респ. Беларусь и Министерства связи и информатизации Респ. Беларусь, 19 февр. 2015 г., № 6/8 // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2015.

8. О мерах по совершенствованию использования национального сегмента сети Интернет: Указ Президента Респ. Беларусь, 1 февр. 2010 г., № 60: в ред. Указа Президента Респ. Беларусь от 23 янв. 2014 г., № 46 // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2015.

9. Дельфинов, А. СМИ: Шпионский скандал может осложнить отношения BND с другими спецслужбами [Электронный ресурс] / А. Дельфинов // Deutsche Welle. – Режим доступа: http:// www.dw.com. – Дата доступа: 11.11.2015.