ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ И ГОСУДАРСТВА В СОВРЕМЕННОМ МИРЕ*

Л.Я. РЖЕУТСКИЙ, старший преподаватель Военной академии Республики Беларусь, полковник юстиции ©

В статье рассмотрены правовые основы информационной безопасности личности и государства в современном мире. Кратко представлены нормативные правовые акты, действующие в Республике Беларусь в данной сфере. Отмечено, что построение нормативного правового механизма закрепляет воздействие информации на основы информационной безопасности личности и государства.

Определено, что в настоящее время уже не существует практического отличия реальной и виртуальной опасности для человека. Проведен анализ законодательства Республики Беларусь и некоторых других государств по защите прав человека на безопасность и личную неприкосновенность, а также общественную безопасность государства в целом. Автор приходит к выводу, что право на безопасность, информационную и личную неприкосновенность – право каждого гражданина, гарантированное Конституцией.

Кроме стремительного роста информационного ресурса, немаловажно ***построение нормативного правового механизма, закрепляющего воздействие информации на основы информационной безопасности личности и государства,*** поскольку информационная безопасность личности – производная от информационной безопасности государства.

О необходимости и возможности превращения экономик отдельных стран в единое мировое хозяйство с постепенным переходом к ***постиндустриальному информационному обществу***, новой экономике, основанной на знаниях, говорится в Программе социально-экономического развития Республики Беларусь на 2006–2010 годы, принятой на третьем Всебелорусском собрании. После подписания Декрета от 22 сентября 2005 года №12 «О парке высоких технологий» «силиконовая долина» в Республике Беларусь становится объективной реальностью»**. Указ Президента Республики Беларусь от 31 января 2006 года №65 «Об утверждении администрации Парка высоких технологий» позволил администрации Парка в августе 2006 года заявить о необходимости создания Академии информационных технологий.

В соответствии с Указом Президента Республики Беларусь от 6 апреля 1999 года №195 «О некоторых вопросах информатизации в Республике Беларусь», постановлением Совета Министров Республики Беларусь от 27 декабря 2002 года №1819 «О государственной программе информатизации Республики Беларусь на 2003–2005 годы и на перспективу до 2010 года «Электронная Беларусь» (далее – Программа) началась реализация данной программы. В документе ставка сделана на ***информационную безопасность республики*** с учетом ***Концепции национальной безопасности.***

Министерство связи и информатизации в марте 2006 года внесло на рассмотрение Правительства обновленный перечень проектов Программы (более 50), реализация которых будет осуществляться в 2006–2010 годах. Основная цель – объединение информационных систем и предоставление многоуровневого права доступа к ним. Обратимся к существующей правовой базе.

Закон от 6 сентября 1995 года «Об информатизации» регулирует правоотношения, возникающие в процессе формирования и использования документированной информации и информационных ресурсов; создания информационных технологий, автоматизированных или автоматических информационных систем и сетей; определяет порядок защиты информационного ресурса, а также прав и обязанностей субъектов, принимающих участие в процессах информатизации. Основу нормативного правового акта представляет порядок пользования документированной информацией, зафиксированной на материальном носителе, с реквизитами, позволяющими ее идентифицировать.

Закон от 10 января 2000 года «Об электронном документе» устанавливает правовые основы применения электронных документов, определяет основные требования, предъявляемые к электронным документам, а также права, обязанности и ответственность участников правоотношений, возникающих в сфере обращения электронных

* Статья поступила в редакцию 31 августа 2006 года.

** Начало обсуждения данной темы см. «Юридический журнал» 2006, №3. С. 44–48.

документов, где электронный документ – информация, зафиксированная на машинном носителе и соответствующая требованиям, установленным настоящим Законом.

Киберпреступность удерживает лидирующие позиции. По данным агентства Associated Press, доходы преступников, совершающих преступления в Интернете, в 2005 году «перешагнули» рубеж в $100 млрд и впервые превысили доходы, получаемые от торговли наркотиками. Масштаб киберпреступности будет расти. Вряд ли найдется сегодня страна, которая могла бы чувствовать себя в безопасности от подобных преступлений (промышленный шпионаж, распространение детской порнографии, пиратство, незаконные операции с ценными бумагами, вымогательство и т.д.). Если в 1998 году террористические организации поддерживали в Интернете 12 сайтов, то в 2006 – до 5 тысяч. При этом абсолютно все крупные террористические структуры активно действуют во Всемирной Сети. К такому выводу пришел известный исследователь терроризма, автор книги «Террор в Интернете» Габриэл Вейманн. Террористические группировки активно используют свои сайты для рекрутирования новых членов и сбора пожертвований. Интернет используется ими для разведывательных целей – по подсчетам Вейманна, в нем содержится до 80% информации, необходимой для организации успешной террористической атаки.

В Республике Беларусь информационной безопасности уделяется значимое внимание. Указом Президента Республики Беларусь от 17 июля 2001 года №390 утверждена Концепция национальной безопасности Республики Беларусь. Документ представляет собой систему взглядов относительно направлений, средств и способов защиты жизненно важных интересов личности, общества и государства, содержит методологическую основу построения системы обеспечения национальной безопасности Республики Беларусь, предназначен для использования при планировании и осуществлении деятельности государственных органов по обеспечению национальной безопасности, где последняя признается одним из приоритетных направлений.

Жизненно важными интересами Республики Беларусь в информационной сфере признаются следующие: обеспечение информационных потребностей личности, общества и государства во всех сферах их жизнедеятельности; обеспечение прав граждан на тайну корреспонденции, телефонных и иных сообщений; эффективное использование национальных информационных ресурсов, создание условий по поддержанию сохранности и систематическому их пополнению; защита сведений, составляющих государственную, служебную, коммерческую и иную охраняемую законодательством тайну; развитие современных информационных технологий, национальной индустрии средств информатизации и связи, расширение участия республики в международной кооперации производителей таких средств и систем; обеспечение безопасности информационных систем и сетей связи; участие Беларуси в работе международных организаций, определяющих принципы и направления сотрудничества в информационной области.

Национальным законодательством предусматривается уголовная ответственность за совершение ряда преступных деяний в области информационной безопасности. Уголовным кодексом Республики Беларусь (далее – УК) предусмотрена уголовная ответственность за хищение путем использования компьютерной техники (ст. 212); несанкционированный доступ к компьютерной информации (ст. 349); модификация компьютерной информации (ст. 350); компьютерный саботаж (ст. 351); неправомерное завладение компьютерной информацией (ст. 352); изготовление или сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353); разработка, использование или распространение вредоносных программ (ст. 354); нарушение правил эксплуатации компьютерной системы или сети (ст. 355). Выявление и пресечение указанных преступлений осуществляется правоохранительными органами путем проведения оперативно-розыскных мероприятий, регулируемых Законом от 9 июля 1999 года «Об оперативно-розыскной деятельности». Статья 11 Закона предоставляет право правоохранительным органам осуществлять контроль почтовых отправлений, телеграфных и иных сообщений, а также снятие информации с технических каналов связи.

Согласно статье 14 Закона от 3 декабря 1997 года «Об органах государственной безопасности Республики Беларусь» Комитет государственной безопасности Республики Беларусь имеет право безвозмездно получать от государственных органов, предприятий, учреждений и организаций, независимо от форм собственности, информацию, необходимую для выполнения возложенных на него задач, а также иметь беспрепятственный доступ к их информационным системам и базам данных в установленном законодательством порядке. В соответствии со статьей 17 Закона юридические и физические лица, оказывающие услуги всех видов электросвязи (за исключением ведомственных и иных систем, не имеющих выхода на сеть общего пользования), обязаны по требованию КГБ включать в состав аппаратных средств сертифицированное дополнительное оборудование и программные средства, а также обеспечить, при наличии санкции прокурора, доступ к специальному оборудованию для снятия информации с каналов связи, а также создавать другие условия, необходимые для проведения органами государственной безопасности оперативно-розыскных мероприятий.

Согласно статье 12 Закона «О единой государственной системе регистрации и учета правонарушений» (вступил в силу 1 января 2007 г. – *ред.*) сведения о правонарушениях, хранящиеся в едином государственном банке данных о правонарушениях, органами внутренних дел предоставляются: органам уголовного преследования, органам, ведущим административный процесс, судам – на основании запроса в течение 5 суток со дня его поступления; другим государственным органам и иным организациям, а также физическим лицам – в течение 10 суток; государственным органам, иным организациям иностранных государств и международным организациям – в соответствии с международными договорами Республики Беларусь.

В целях обеспечения информационной безопасности действует Закон от 15 декабря 2005 года «О внесении дополнений и изменений в некоторые законодательные акты Республики Беларусь по вопросу усиления ответственности за деяния, направленные против человека и общественной безопасности». В Законе определены меры уголовной ответственности за дискредитацию Республики Беларусь – предоставление иностранному государству, иностранной или международной организации заведомо ложных сведений о политическом, экономическом, социальном, военном или международном положении Республики Беларусь, правовом положении граждан в Республике Беларусь, дискредитирующих Республику Беларусь или ее органы власти.

В январе 2006 года Минсвязи и МВД подписали совместное постановление о взаимодействии органов внутренних дел и мобильных операторов. Подобная законодательная практика существует во многих государствах. В частности, УК ФРГ предусматривает ответственность за так называемый изменнический подлог (§ 100а): *«Кто делает доступным для другого лица или общественности заведомо поддельные или фальсифицированные предметы, сведения о них или ложные утверждения фактического характера, которые в случае их подлинности или истинности имели бы значение для внешней безопасности или для отношений Федеративной Республики Германии с другой страной, чтобы умышленно ввести в заблуждение иностранное государство, что якобы речь идет о подлинных предметах или фактах, и создать этим опасность причинения серьезного вреда внешней безопасности или отношениям Федеративной Республики Германии с иностранным государством, наказывается лишением свободы на срок от шести месяцев до пяти лет...».* Статья 133 УК Польши предусматривает за публичное оскорбление нации или Республики Польша наказание в виде лишения свободы на срок до 3 лет. В § 1001 (титул 18) Свода законов США зафиксировано: *«Тот, кто по какому-либо вопросу, относящемуся к компетенции какого-либо ведомства или агентства Соединенных Штатов, заведомо и умышленно фальсифицирует или скрывает при помощи уловки, хитрости или обмана какой-либо факт, делает ложное или фиктивное заявление либо изготавливает или использует какой-то документ, зная, что таковой содержит ложное или фиктивное заявление или запись, наказывается штрафом до 10.000 долларов или тюремным заключением на срок до пяти лет либо подвергается обоим наказаниям».* Уголовные законы большинства стран мира защищают государство в целом и отдельные его структуры от недостоверной информации.

В ближайшее время будет создана база данных о терроризме, охватывающая все страны Евросоюза. Единая информационная база нормативных правовых актов государств-участников СНГ в сфере противодействия терроризму, незаконному обороту наркотических средств, психотропных веществ и их прекурсоров и иным видам преступлений будет создана уже в 2007 году. Проект соглашения о создании такой базы обсудили члены рабочей экспертной группы на заседании, прошедшем 11–13 апреля 2006 года в Исполнительном комитете СНГ в Минске.

10 марта 2006 года в России вступил в силу Закон «О мерах по противодействию терроризму». Под терроризмом в нем понимается идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и иными формами противоправных насильственных действий. Государственная Дума приняла также проект Закона «О персональных данных», рассматривающего порядок сбора, использования и защиты информации.

В Республике Беларусь в первом полугодии 2006 года создано предприятие по сопровождению государственных информационных ресурсов и систем. Являясь держателем Регистра населения (базового информационного ресурса страны), оно станет связующим звеном между другими ресурсами органов госуправления и организаций.

Интересен опыт ряда зарубежных стран. Особый путь у некоторых стран Европы. Согласно Закону «О контртеррористической деятельности и борьбе с организованной преступностью», одобренному Сенатом Бельгии, полицейские могут, например, производить скрытое визуальное наблюдение за подозреваемыми в причастности к террористической деятельности практически везде, за исключением мест их постоянного проживания. Им разрешено в случае необходимости проводить у подозреваемых обыски в любое время суток.

Услуга мониторинга местонахождения владельцев сотовых телефонов пользуется все большей популярностью в Великобритании. Отслеживать владельца того или иного сотового телефона руководство компаний берется по разным причинам, и услуги отслеживания никак не ограничивают свое наблюдение только лишь рабочим днем.

По данным Центра деловой этики при колледже Бентли, примерно 92% американских компаний используют видеокамеры для наблюдения за посетителями и сотрудниками и после окончания рабочего дня, используя Системы Глобального Позиционирования (GPS). Под лозунгом борьбы с терроризмом Министерство обороны США объявило конкурс на разработку детектора лжи, который позволил бы дистанционно отслеживать психическое состояние людей таким образом, что никто даже не будет подозревать об этом. В январе 2006 года ученые Колумбийского университета заявили, что детектор лжи нового поколения создан. В основе новой технологии – последние открытия в области нейрохирургии и анализа работы человеческого мозга.

Ведущие банки мира в течение ближайших пяти лет могут начать использовать чеки с дактилоскопической защитой, сообщила фирма Accenture на презентации, которая состоялась в январе 2006 года, посвященной банкам будущего. Было обращено внимание на такое нововведение, как радиочастотная идентификация (RFID). Клиенты могут автоматически идентифицироваться RFID-кодированными картами, находящимися в их бумажниках, когда они проходят через двери банков.

Для личности и государства опасен и экстремизм. Рабочая группа Постоянной комиссии Парламента по национальной безопасности Республики Беларусь в апреле 2006 года рассмотрела законопроект о противодействии экстремизму. В проекте дано **определение понятия «экстремистская деятельность»**. Это действия, направленные на подрыв национальной безопасности государства; насильственное изменение конституционного строя; захват либо удержание государственной власти неконституционным путем; создание незаконных вооруженных формирований; осуществление террористической деятельности; разжигание расовой, национальной, религиозной вражды и социальной розни; организация массовых беспорядков, а также публичные призывы к указанной деятельности, ее финансирование или иное содействие в осуществлении, в том числе путем предоставления недвижимости, учебной, полиграфической и другой материально-технической базы, средств электросвязи, информационных услуг.

Преступность оказывает дестабилизирующее воздействие на состояние всех сфер жизнедеятельности государства, общества и личности. Указом Президента Республики Беларусь от 21 февраля 2006 года №103 утверждена Государственная программа о борьбе с преступностью на 2006–2010 годы. В ней существенное внимание уделено информационной безопасности личности и государства.

В частности, обозначим лишь некоторые ***мероприятия, способствующие реализации права на безопасность в среде информационных технологий:*** выявление и пресечение преступлений с использованием компьютерных технологий (ст. 21.9); внедрение в деятельность правоохранительных, судебных органов и судебно-экспертных учреждений и подразделений информационно-поисковой системы «Аипсин» (ст. 33.1); внедрение в деятельность правоохранительных органов биометрической системы автоматизированной идентификации и контроля (ст. 33.2); модернизация системы передачи извещений о проникновении на охраняемый объект и пожаре АСОС «Алеся» (ст. 33.4); обеспечение регулярного освещения в средствах массовой информации деятельности правоохранительных и контролирующих органов по борьбе с преступностью и защите граждан от преступных посягательств (ст. 38); продолжение работы по созданию и внедрению систем радиоохраны для обеспечения охраны нетелефонизированных объектов, квартир и жилых домов граждан (ст. 42.3); создание системы обеспечения безопасности граждан и транспортных средств, находящихся в личном пользовании, на базе современных навигационно-информационных технологий (ст. 42.4); способствование созданию единого информационного банка данных МВД Республики Беларусь и МВД Российской Федерации о лицах, причастных к совершению преступлений в сфере высоких технологий (ст. 44.7); разработка автоматизированной системы передачи информации о лицах, причастных к международным террористическим организациям, розыскиваемых за совершение преступлений, с целью выявления указанных лиц в пассажиропотоке и организации предупреждения использования ими авиационного транспорта (ст. 44.8).

В плане информационной защиты личности и государства очень важно соблюдение конституционного ***права на личную неприкосновенность.*** В декабре 2005 года Верховный комиссар ООН по правам человека Луиза Арбур, выступая на пресс-конференции в штаб-квартире ООН в Нью-Йорке, предупредила, что готовность принести все традиционные демократические свободы на алтарь безопасности может привести к созданию мира, в котором не будет ни безопасности, ни свободы.

Конституция Республики Беларусь предоставляет гарантии на защиту от незаконного вмешательства в личную жизнь, в том числе от посягательства на тайну корреспонденции, телефонных и иных сообщений, на честь и достоинство. Закон «О связи» гарантирует тайну корреспонденции, телефонных и других сообщений. Для работников предприятий связи устанавливается обязанность сохранять тайну переписки лиц, пользующихся услугами связи, не нарушать тайну телефонных разговоров, телеграфных и других сообщений (ст. 11).

Закон «О печати и других средствах массовой информации» гарантирует гражданам свободу печати и других СМИ. Граждане Республики Беларусь имеют право учреждать средства массовой информации, владеть, пользоваться и распоряжаться ими, а также беспрепятственно искать, получать,

использовать и распространять информацию при их помощи, свободно выражать через них свои мысли, взгляды и убеждения (ст. 3 Закона).

Согласно статье 19 Закона от 6 сентября 1995 года «Об информатизации» органы государственной власти, юридические и физические лица имеют равные права на доступ к информационным ресурсам. Порядок доступа к открытой документированной информации определяется ее собственником или уполномоченным им лицом на основании договора или в порядке исполнения служебных обязанностей. Органы государственной власти обязаны организовать работу по формированию информационных ресурсов, являющихся собственностью государства, а также обеспечить предоставление доступа к открытым информационным ресурсам, являющимся собственностью государства, всем заинтересованным лицам (ст. 20). ***Законодательством не допускается сбор, хранение, использование информации о личной жизни граждан без их согласия.***

Общеевропейское законодательство также имеет несколько документов, регулирующих данную сферу. Так, статья 10 Европейской конвенции по правам человека гарантирует право на получение и передачу информации. Рекомендация Совета Европы R (81) 19 от 25 ноября 1981 года «О доступе к информации, находящейся в ведении государственных ведомств» содержит ряд основополагающих принципов. Например, все государства – члены Совета Европы должны обеспечивать право на получение по запросу информации, находящейся в ведении государственных органов (за исключением законодательных и судебных органов), и обязуются реализовать эффективные и должные меры по обеспечению доступа к информации. При этом допускаются лишь четко определенные ограничения и исключения, связанные с обеспечением конфиденциальности охраняемых видов информации, разглашение которой в соответствии с законом не может быть осуществлено в обычном порядке.

Такую ***охраняемую информацию*** можно подразделить на шесть основных видов: государственная тайна; служебная тайна; коммерческая тайна; банковская тайна; профессиональная тайна и тайна личной жизни. В отношении первых пяти видов законодательством Республики Беларусь урегулирован порядок обращения с ними. Пока граждане не получат каких-либо действенных механизмов защиты своих персональных данных, в условиях стремительного развития информационно-технических технологий это фактически может привести к нарушениям прав на неприкосновенность личной жизни, сделав ее неоправданно прозрачной. Нецелевое использование персональных данных может нанести огромный и непоправимый вред человеку.

Существуют ряд «антипримеров», где посредством СМИ осуществляется попытка контроля и профилактики возможного преступного поведения граждан. В Лондоне начал работу телеканал Shoreditch TV, который транслирует видеозаписи с камер наружного наблюдения, установленных на улицах города. Проект запущен под лозунгом «Боритесь с преступностью, сидя на диване». Подписчикам предлагается отправить в полицию анонимное электронное письмо, если они заметят на экране что-то подозрительное. Shoreditch TV демонстрирует кадры с 400 камер в лондонском Ист-Энде. Каждому подписчику предоставляют доступ к базе данных с именами и фотографиями британцев, которые попали под наблюдение полиции за нарушения общественного порядка и мелкие преступления. Таким образом осуществляется попытка тотального контроля граждан друг за другом.

Первой страной, закрепившей право общественности на доступ к официальной информации, была Швеция, в 1766 году принявшая соответствующий закон. В некоторых странах также приняты специализированные законы: в Бельгии – «О гласности в сфере администрации»; в Германии – «Об ознакомлении с официальными документами и о доступе к информации»; в Норвегии – «Об общественном доступе к документам»; в США – «О свободе информации»; в Швейцарии – «Об информировании общественности». Подобные законы имеют Франция, Великобритания, Испания, Венгрия. В Кыргызской Республике действует Закон «О гарантиях и свободе доступа к информации», в Эстонии – «О публичной информации», в Узбекистане – «О гарантиях и свободе доступа к информации».

Таким образом, информационная безопасность личности и государства находится в неразрывном единстве и является главной составной частью безопасности как непременном условии сохранения современного мира.

SUMMARY

The article considers legal bases of information safety of the person and the state in the modern world. The normative legal certificates working in Byelorussia in the given sphere are briefly submitted. It is marked that the construction of a normative legal mechanism fixes the influence of information on bases of information safety of the person and the state.

It is determined, that now there is no any more practical difference of real and virtual danger to the person. The brief analysis of the legislation of Byelorussia and some other states on protection of human rights on safety and inviolability of person, and also public safety of the state as a whole is lead. The following conclusion is made: information safety of the person – a derivative from information safety of the state. The right on safety, including information, inviolability of a person – the personal right of the citizen, a gain guaranteed by the Constitution.