УДК 004:34

С.В. Козлов, Т.Г. Чудиловская

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В условиях стремительного развития информационно-телекоммуникационных технологий проблема обеспечения информационной безопасности личности, в том числе предотвращения незаконных действий с информацией персонального характера, приобрела особое значение. Персональные данные относятся к категории конфиденциальной информации, предполагающей отсутствие свободного доступа к ней и наличие эффективной системы ее защиты. Меры по обеспечению безопасности и предотвращению незаконных действий с персональными данными получили легальное обозначение в виде понятия «защита персональных данных».

В решение вопросов обеспечения эффективного механизма защиты персональных данных призвана внести свой вклад и юридическая наука.

Анализ белорусского законодательства в области персональных данных и практики его применения показывает наличие пробелов в правовом регулировании в сфере персональных данных.

Среди основных проблем, существующих в настоящее время в сфере защиты персональных данных, можно выделить следующие:

1. Отсутствие в национальном законодательстве единого согласованного подхода к определению понятия «персональные данные». Общественные отношения в сфере персональных данных регулируют нормы Закона от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» и Закона от 21 июля 2008 г. № 418-З «О регистре населения», а также отдельные предписания других нормативных правовых актов. Эксперты обращают внимание на то, что определения, которые содержатся в вышеуказанных законах, имеют разный объем содержания. Базовый закон в сфере информатизации и защиты информации «Об информации, информатизации и защите информации» не раскрывает значение термина «персональные данные». Вместе с тем в нем закреплены основы правового регулирования отношений, связанных с защитой персональных данных. Для целей Закона «О регистре населения» персональные данные определены как совокупность основных и дополнительных персональных данных, а также данных о реквизитах документов, подтверждающих основные и дополнительные персональные данные конкретных физических лиц. Такая несогласованность ключевого определения приводит к невозможности единообразного подхода к правовому регулированию этой сферы.

2. Несоответствие требований защиты персональных данных принципам Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (заключена в Страсбурге 28 января 1981 г.). Установленные Конвенцией основные права и свободы граждан в сфере защиты персональных данных (право на защиту своих персональных данных, право иметь доступ к своим персональным данным, право изменять и дополнять свои персональные данные и т. д.), основополагающие принципы защиты персональных данных (ограничение к обработке персональных данных о национальной принадлежности, политических взглядах, религиозных убеждениях и т. д.) могут быть использованы при дальнейшей разработке законодательства Республики Беларусь по защите персональных данных.

3. Отсутствие в белорусском законодательстве специальных мер ответственности за незаконное распространение и использование персональных данных. Кодекс Республики Беларусь об административных правонарушениях и Уголовный кодекс Республики Беларусь содержат ряд составов противоправных деяний в области информационной безопасности и защиты информации, предусматривающих ответственность за нарушение режима ограниченного доступа и конфиденциальности в отношении информации. Однако необходимость введения соответствующих специальных норм объективно существует.

4. Законодательными актами не урегулирован детальный порядок работы с персональными данными: не определен четкий порядок подготовки и направления запроса на предоставление персональных данных, их сбора, обработки, хранения, распространения и предоставления, отсутствуют единообразные подходы к установлению сроков хранения персональных данных.

5. Не определен правовой статус субъектов, участвующих в обороте персональных данных, их права и обязанности. Это является одним из важнейших инструментов поддержания баланса защищаемых законом ценностей и интересов гражданина, общества и государства в процессе оборота персональных данных.

6. Отсутствие четкой регламентации сбора, хранения, обработки и использования персональных данных коммерческими структурами. Законы Республики Беларусь концентрируются главным образом на защите персональных данных, которые находятся в распоряжении государственных органов. Требования к бизнес-структурам заключаются прежде всего в технических стандартах информационной безопасности и отраслевых нормативных актах.

Отечественные правоведы отмечают, что насущной задачей является совершенствование законодательства о персональных данных и прежде

всего разработка и принятие закона (либо концепции) о защите персональных данных, устанавливающего унифицированные правила сбора и обработки персональных данных физических лиц, а также возникающие при этом правовые механизмы защиты прав граждан.

Целесообразным видится разработка и принятие закона Республики Беларусь «О персональных данных», который должен комплексно регламентировать вопросы правового регулирования и защиты персональных данных, закрепить единое определение понятия «персональные данные», выделить категории общедоступных персональных данных и конфиденциальных персональных данных с установлением их правового режима, обозначить условия и порядок получения, передачи, сбора, хранения, обработки и предоставления персональных данных, предусмотреть права и обязанности лиц, чьи персональные данные обрабатываются, и субъектов, осуществляющих обработку персональных данных, закрепить иные положения.

Предлагаемый закон позволит определить общие подходы к обработке персональных данных в нашей стране, устранить существующие пробелы в правовом регулировании персональных данных, а также обеспечить соблюдение конституционного права гражданина на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство и иные персональные данные.

УДК 002.004.056

Э.П. Крюкова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Несанкционированный доступ к информации, относящейся к критически важным объектам (КВО), способствует ее успешному использованию при организации саботажа в отношении критических активов КВО, террористических актов, вмешательству в работу компьютерных систем управления безопасностью и технологическими процессами, компьютерных систем физической защиты и другим противоправным действиям.

На понимание потенциальных угроз КВО критических инфраструктур значительно повлияло изменение масштаба и границ международного терроризма, использующего самые передовые информационные технологии для организации диверсий и атак. Это привело к необходи-

мости решения проблемы защиты информации на КВО, т. е. обеспечения его информационной безопасности.

Стала очевидной одна из самых существенных угроз безопасности КВО – легкая доступность для потенциальных атакующих информации о важных технологических процессах, компьютерных системах контроля и управления; других активах, важных для безопасности КВО, зонах их размещения; системе физической защиты, системах, обеспечивающих непрерывность функционирования; ключевом персонале, особенностях организационного управления объектом и др.

Защита информации о таких активах является важной задачей, и управление ими требует особого подхода к реализации организационных и технических мероприятий по обеспечению безопасности КВО.

К охраняемой информации на КВО критической инфраструктуры относится информация, нарушение конфиденциальности, целостности или доступности которой может создать угрозу нарушения нормального функционирования и (или) нарушения безопасности КВО. Охраняемая информация на КВО включает:

бизнес-информацию;

техническую информацию;

технологическую (оперативную) информацию (данные), генерируемую в ходе технологических процессов;

информацию о КВО, представленную на сайте и в средствах массовой информации.

При организации защиты информации на КВО должны рассматриваться две основные группы взаимосвязанных целей:

информационная безопасность КВО – обеспечение конфиденциальности, целостности, доступности информации (защита критической информации на КВО);

компьютерная безопасность КВО – обеспечение целостности, доступности информации, которая генерируется в ходе технологических процессов и преобразуется компьютерными системами в команды для управления программно-аппаратными средствами и в информацию для принятия решений оператором (защита компьютерных систем, обрабатывающих критическую информацию).

В настоящее время в связи с участившимися сетевыми атаками на системы контроля и управления критически важными инфраструктурами выделяется новое направление в обеспечении компьютерной безопасности КВО – кибернетическая безопасность. Обеспечение кибернетической безопасности КВО требует:

повышения готовности к сетевым компьютерным атакам, снижения времени реагирования механизмов защиты на инциденты, разработки