

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. Ю. Чешко

*Белорусский государственный университет,
ул. Ленинградская 8, 220030, г. Минск, Беларусь, vladimir_cheshkos@mail.ru*

В статье рассматривается правовое регулирование системы информационной безопасности, выделяются отдельные проблемы в данной сфере. Обосновывается необходимость закрепления правового статуса службы информационной безопасности, совершенствование механизма обеспечения защиты персональных данных, а также усиление ответственности для должностных лиц государственных органов за необеспечение информационной безопасности.

Ключевые слова: система информационной безопасности; правовое регулирование; юридическая ответственность; защита персональных данных.

PARTICULAR PROBLEMS OF LEGAL REGULATION OF THE INFORMATION SECURITY SYSTEM

V. Yu. Cheshko

*Belarusian State University,
Leningradskaya st. 8, 220030, Minsk, Belarus, vladimir_cheshkos@mail.ru*

The article considers the legal regulation of the information security system, highlights certain problems in this area. The need to consolidate the legal status of the information security service, improve the mechanism for ensuring the protection of personal data, as well as strengthen responsibility for officials of state bodies for failure to ensure information security is justified.

Keywords: information security system; legal regulation; legal liability; personal data protection.

Информационная безопасность представляет собой состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Правовой основой для обеспечения информационной безопасности выступает Конституция Республики Беларусь. В ней определено, что

государство обеспечивает свободу, неприкосновенность и достоинство личности. Ограничение или лишение личной свободы возможно в случаях и порядке, установленных законом;

каждый имеет право на защиту от незаконного вмешательства в его частную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство. Государство создает условия для защиты персональных данных и безопасности личности и общества при их использовании;

гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, о политической, экономической, культурной и международной жизни, состоянии окружающей среды. Государственные органы, должностные лица обязаны предоставить гражданину Республики Беларусь возможность ознакомиться с материалами, затрагивающими его права и законные интересы. Пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, частной и семейной жизни граждан и полного осуществления ими своих прав [1, ст. 25, 28, 34].

Анализ правового регулирования показывает наличие следующей системы нормативных правовых актов, устанавливающих основу информационной безопасности в Республике Беларусь:

1) Закон Республики Беларусь от 10.11.2008 г. № 455-3 «Об информации, информатизации и защите информации» [2];

2) Концепция национальной безопасности Республики Беларусь, утвержденная Указом Президента Республики Беларусь от 09.11.2010 г. № 575 (далее – Концепция национальной безопасности) [3];

3) Концепция информационной безопасности Республики Беларусь, утвержденная Постановлением Совета Безопасности Республики Беларусь от 18.03.2019 г. № 1 (далее – Концепция информационной безопасности) [4].

Представленная система правового регулирования обеспечения информационной безопасности свидетельствует о том, что в Республике Беларусь имеется существенная правовая основа для обеспечения информационной безопасности, приняты как концептуальные акты, так и нормативные правовые акты, регулирующие данную сферу общественных отношений.

Переходя к анализу проблем в данной сфере следует изначально определить, что рассматриваться будут только проблемы организационно-правового характера. В ходе исследования правового регулирования системы обеспечения информационной безопасности следует выделить

следующие направления совершенствования законодательства в данной сфере:

правовой статус сотрудников службы информационной безопасности;

порядок правового обеспечения защиты персональных данных;

ответственность в сфере информационной безопасности.

Правовой статус сотрудников службы информационной безопасности. Правовой статус – это совокупность элементов, характеризующих правовое положение субъекта, которое отражает его фактическое состояние во взаимоотношениях с обществом, другими объектами и государством. Правовой статус отражает юридически оформленные взаимоотношения личности и общества, гражданина и государства, отдельного индивида с окружающими. В нем выражаются легальные пределы свободы личности, объем ее прав, обязанностей, других правовых возможностей и ответственности. В структуру правового статуса, как правило, включают следующие элементы: права; обязанности; ответственность.

В настоящее время в различных государственных органах и иных организациях существуют определенные структурные подразделения и должностные лица, осуществляющие обеспечение информационной безопасности. Однако для системной работы по эффективному обеспечению информационной безопасности на различных уровнях полагаем целесообразным разработать типовое положение о службе информационной безопасности. Полагаем, что такой акт следует принять в форме постановления Совета Министров Республики Беларусь и распространить на все республиканские органы государственного управления. В данном положении предусмотреть следующие разделы:

общие положения. Определить, что служба информационной безопасности является структурным подразделением государственного органа (организации), создаваемая (учреждаемая) в целях обеспечения информационной безопасности его деятельности;

структура службы информационной безопасности;

задачи службы информационной безопасности. К задачам отнести разработку и реализацию политики информационной безопасности, контроль за обеспечением организации технических средств защиты информации и их функционированием, проведение контрольных мероприятий, реагирование на различные угрозы информационной безопасности и др.;

права, обязанности и ответственность сотрудников службы информационной безопасности.

Порядок правового обеспечения защиты персональных данных. В Законе Республики Беларусь от 7 мая 2021 г., № 99-З «О защите персональных данных» регулирует данный вопрос. Подход, заложенный в этот

нормативный правовой акт, является новым для Республики Беларусь и создает немало проблем по его толкованию и правоприменению.

На наш взгляд, ряд норм этого нормативного правового акта содержит положения, при применении которых достаточно сложно определить их границу. Так, например, в ст. 8 установлены случаи, когда согласие на обработку персональных данных не требуется. В частности, к таким случаям отнесены предусмотренные уголовно-исполнительным законодательством, законодательством в области национальной безопасности, об обороне, о борьбе с коррупцией, о борьбе с терроризмом и противодействии экстремизму, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения, о Государственной границе Республики Беларусь, о гражданстве, о порядке выезда из Республики Беларусь и въезда в Республику Беларусь, о статусе беженца, дополнительной защите, убежище и временной защите в Республике Беларусь [5].

При этом в указанном законе не установлен никакой механизм защиты прав граждан и иных субъектов. В связи с этим полагаем, что следует определить порядок обжалования данных решений в случае существенных нарушений персональных данных пользователя, либо при наличии совершенного в связи с этим преступления или административного правонарушения.

Ответственность в сфере информационной безопасности. Следует отметить, что, исходя из публичных начал обеспечения защиты информационной безопасности государства и общества, в данном вопросе внимание будет уделено уголовной и административной ответственности в сфере обеспечения информационной безопасности.

Преступления в данной сфере закреплены в гл. 31 УК и включают 5 статей [6]. Среди них: Несанкционированный доступ к компьютерной информации (ст. 349); Модификация компьютерной информации (ст. 350); Неправомерное завладение компьютерной информацией (ст. 352); Разработка, использование либо распространение вредоносных программ (ст. 354); Нарушение правил эксплуатации компьютерной системы или сети (ст. 355).

Кроме того, к преступлениям данной сфере следует отнести также следующие составы, закрепленные в УК: хищение путем использования компьютерной техники (ст. 212); причинение имущественного ущерба без признаков хищения (ст. 216, путем модификации компьютерной информации). Отдельную группу преступлений включают преступления, связанные с содержанием компьютерных данных: детская порнография, нарушение авторского права.

В Беларуси установлены широкие запреты в отношении всех порнографических материалов. В ст. 343 и ст. 343-1 УК распространение порнографических материалов посредством сети Интернет является квалифицирующим признаком (ст. 343 УК. Изготовление и распространение порнографических материалов или предметов порнографического характера).

В отношении нарушений авторских прав с использованием компьютерных технологий уголовное право Республики Беларусь не предусматривает каких-либо специальных норм.

Данная категория административных правонарушений предусмотрена гл. 23 КоАП, которая включает в себя 10 статей [7].

Родовым объектом этих правонарушений являются регулируемые законодательством общественные отношения в сфере связи и информации. Вместе с тем, дополнительными объектами по отдельным составам могут быть: общественный порядок и общественная безопасность (части 4 и 5 ст. 23.5); отношения интеллектуальной собственности (ст. 23.6); права и свободы физического лица (ст. 23.7); установленный законодательством порядок управления (ст. 23.8); отношения в сфере хозяйственной деятельности (ч. 1 ст. 23.9).

Исходя из анализа норм по уголовной и административной ответственности можно сделать вывод, что в Республике Беларусь имеется значительное правовое регулирование по защите информационной безопасности государства, общества и человека, однако, на наш взгляд, имеется направление для его совершенствования. Наиболее существенный вред в сфере обеспечения информационной безопасности может быть причинен непосредственно должностным лицом государственного органа, как правило, правоохранительного. Это обусловлено тем, что в ходе осуществления своей деятельности данная категория обладает достаточно простым и неограниченным доступом к различным информационным системам и, соответственно, может их использовать в целях, не предназначенных для этого. Наглядным примером выступает Российская Федерация, где за денежные средства можно приобрести практически любую ценную информацию из закрытых информационных ресурсов государственных органов. В связи с этим, полагаем, что для повышения эффективности обеспечения информационной безопасности УК и КоАП необходимо дополнить составами о нарушении информационной безопасности должностным лицом государственного органа и предусмотреть ответственность за это гораздо серьезнее, чем за должностные преступления и правонарушения.

Таким образом, по результатам рассмотрения проблем правового регулирования в системе обеспечения информационной безопасности можно сделать следующие выводы:

для системной работы по эффективному обеспечению информационной безопасности на различных уровнях полагаем целесообразным разработать типовое положение о службе информационной безопасности. Полагаем, что такой акт следует принять в форме постановления Совета Министров Республики Беларусь и распространить на все республиканские органы государственного управления;

в Законе «О защите персональных данных» не установлен никакой механизм защиты прав граждан и иных субъектов в случаях, когда согласие на обработку их персональных данных не требуется. В связи с этим полагаем, что следует определить порядок обжалования данных решений в случае существенных нарушений персональных данных пользователя, либо при наличии совершенного в связи с этим преступления или административного правонарушения;

для повышения эффективности обеспечения информационной безопасности в УК и КоАП необходимо дополнить составами о нарушении информационной безопасности должностным лицом государственного органа и предусмотреть ответственность за это гораздо серьезнее, чем за должностные преступления и правонарушения.

Библиографические ссылки

1. Конституция Республики Беларусь 1994 года : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г и 27 фев. 2022 г. Минск : НЦПИ, 2022. С. 80.

2. Об информации, информатизации и защите информации : Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З : в ред Закона от 10.10.2022 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.

3. Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 : в ред Указа Президента Респ. Беларусь от 24.01.2014 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.

4. О концепции информационной безопасности Республики Беларусь : постановление Совета Безопасности Респ. Беларусь, 18 мар. 2019 г., № 1 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.

5. О защите персональных данных: Закон Респ. Беларусь, 7 мая 2021 г., № 99-З : в ред Закона от 01.06.2022 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.

6. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 09.03.2023 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.

7. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 янв. 2021 г., № 91-З : принят Палатой представителей 18 дек. 2020 г. : одобр. Советом Респ. 18 дек. 2020 г. : в ред. Закона Респ. Беларусь от 09.12.2022 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.