УДК 004.056(575.1)

НОРМАТИВНО-ПРАВОВЫЕ ВОПРОСЫ УКРЕПЛЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Х.К. САМАРОВ

Ташкентский университет информационных технологий имени Мухаммада-аль Хоразмий, Республика Узбекистан

Поступила в редакцию 20 марта 2019

Аннотация. В статье рассматриваются нормативно-правовые аспекты укрепления кибербезопасности в республике Узбекистан.

Ключевые слова: информационная система, информационный ресурс, информационная безопасность, кибербезопасность.

В свете развития информационных технологий все большую актуальность обретает проблема укрепления кибербезопасности. Данный вопрос неоднократно поднимается и главами государств. Так, Президент Республики Узбекистан в начале 2018 г. подписал Указ «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», в котором особое внимание уделяется реализации комплексных мер по обеспечению кибербезопасности и внедрению современных технологий защиты сетей, программных продуктов, информационных систем и ресурсов, участию в регулировании применения технологий сбора, обработки и хранения персональных и биометрических данных.

На сегодняшний день, ввиду стремительного распространения информационных сетей, актуальным является вопрос обеспечения надлежащего уровня кибербезопасности. При этом в условиях наличия активной угрозы нарушения прав и свобод граждан и организаций государству необходимо постоянно совершенствовать организационные, правовые и инженерно-технические механизмы контроля в отношении сетей телекоммуникаций. Ситуация осложняется тем, что на сегодняшний день активное участие в кибератаках, незаконном сборе информации о государственных служащих, корпорациях и простых гражданах принимают государственные структуры развитых стран. При этом применяются и различные методы манипуляция людьми при помощи сети Интернет [1]. Опыт последних лет указывает, что киберпреступность перешагнула границы отдельных государств и стала международной.

Лидерство в киберпространстве является и одним из приоритетов США. Американская национальная стратегия безопасности строится на дипломатии, разведке, военном комплексе, правоохранительных органах, а также экономических инструментах [2].

Однако самые эффективные методы защиты информационных данных и обеспечения кибербезопасности существуют в КНР. С 2003 г. в КНР действует проект «Золотой щит», который также называют «Великим китайским файерволом», так как большая часть его задач заключается в блокировке ненадежных сайтов и IP-адресов. Доступ к иностранным сайтам изнутри материкового Китая ограничивается правительством Китая. Веб-страницы фильтруются по ключевым словам, связанным с государственной безопасностью, а также по «черному списку» адресов сайтов. К инструментам работы «Золотого щита» можно отнести блокировку по IP адресу, DNS, URL, TCP фильтры, блокираторы подключения, создание фальшивых SSL подключений.

Закон КНР «О кибербезопасности» от 7 ноября 2016 г. (далее – Закон КНР 2016 года) предусматривает проведение ежегодных оценок рисков кибербезопасности и предоставление отчетов о результатах этих оценок и мерах по улучшению ситуации соответствующим органам власти (статья 38). Цель контроля над сетью Интернет в КНР – предотвратить проникновение нежелательной информации внутрь страны и утечку информации за рубеж, в том числе путем блокирования информационных ресурсов и поисковых систем [3].

Впрочем, опыт КНР в сфере обеспечения информационной безопасности часто подвергается критике, и является наиболее радикальным. Фактически специалисты КНР оградили свою часть глобальной сети «железным щитом» путем фильтрации любой информации, которая как поступает к ним, так и исходит от них.

Следует отметить, что, несмотря на законодательное урегулирование в Республике Узбекистан вопроса обеспечения кибербезопасности, эффективному процессу построения системы защиты информационного пространства препятствует ряд проблемных вопросов, требующих государственного урегулирования.

К таким вопросам можно отнести вопросы контроля над сетями телекоммуникаций, многие из которых находятся в частной собственности, вопросы защиты секретной информации, а также личных данных граждан Узбекистана, уязвимости в отечественных системах защиты информационных ресурсов.

Конвенция Совета Европы о киберпреступности разделила киберпреступность на четыре группы (дополнительный протокол добавил пятую группу) [4]. На сегодняшний день ряд государств успешно проводит политику укрепления информационной безопасности.

Исходя из международного опыта можно выделить три основные модели правового регулирования распространения информации в сети Интернет [5]. Первая модель предусматривает полный контроль государством над сетью Интернет. Данной модели придерживается, к примеру, КНР, где практически вся сеть Интернет находится под полным государственным контролем.

Вторая модель предусматривает ответственность провайдера за любые действия пользователя. Третья модель регулирования безопасности в сети Интернет предусматривает освобождение провайдера от ответственности в тех случаях, если он выполняет определенные условия, связанные с характером предоставления услуг и взаимодействия с субъектами информационного обмена.

Ключевым вопросом обеспечения информационной безопасности Республики Узбекистан является вопрос контроля над хранением и распространением информации. Информация, распространяемая в сетях телекоммуникаций, включает в себя как персональные данные пользователей, так и государственные секреты и закрытую информацию. Поэтому так важно иметь достаточную правовую основу для создания стабильной системы в сфере хранения и распространения информации.

Анализ законодательства в сфере хранения и распространения информации выявил ряд проблемных вопросов, которые требуют принятия мер для их последующего решения. Во-первых, на сегодняшний день источники угроз информационной безопасности могут находиться вне юрисдикции законодательства Республики Узбекистан, что существенно затрудняет применение системы правовых мер. Во-вторых, в соответствии с пунктом 1 статьи 18 Закона Республики Узбекистан «О телекоммуникациях», операторы связи и (или) владельцы сетей связи обязаны осуществлять содействие в сборе и хранении служебной информации в порядке, определяемом органами, проводящие оперативно розыскную деятельность. Однако закон не предписывает осуществлять сбор и хранение данных пользователей (переписка, звонки и т. д.). Для сравнения, в законе КНР «О мерах по регулированию информационных услуг через Интернет» от 1 октября 2000 г. предусмотрено, что провайдеры должны хранить такую информацию в течение времени, на которое его подписчики получают выход в Интернет, номера счетов подписчиков, адреса или названия доменов веб-сайтов и основные телефонные номера, которые они используют в течение 60 дней (статья 14). В-третьих согласно пункту 9 статьи 6 Закона Республики Узбекистан «Об информатизации» в компетенцию уполномоченного органа входит содействие по защите прав и законных интересов пользователей информационных ресурсов в вопросах безопасного использования информационно-коммуникационных технологий.

Для реализации данной компетенции уполномоченный орган обращается в суд с требованием блокировать те или иные информационные ресурсы, содержащие материалы, противоречащие законодательству Республики Узбекистан (пропаганда экстремизма, разжигание межнациональной розни, распространение порнографии и т. п.).

С 2012 г. в России действует Единый реестр запрещенных сайтов. Реестр – это конкретный набор из ста тысяч адресов. Реестр находится в ведении Роскомнадзора, в соответствии с постановлением Правительства Российской Федерации от 26 октября 2012 г. № 1101.

Необходимо рассмотреть возможность введения аналогичного механизма и в Республике Узбекистан. В целях повышения эффективности, упрощения процедуры и оперативного принятия мер по пресечению распространения незаконного контента предлагается следующее.

1. Упростить процедуры блокировки Интернет-ресурсов, путем возможности самостоятельной блокировки уполномоченным органом без обращения в суд. В качестве варианта можно перенять российский опыт ведения реестра запрещенных сайтов.

2. Распределить функции мониторинга Интернет-пространства между некоторыми государственными органами (например, анализ контента на предмет наличия угроз национальной безопасности отнести к введению органов службы государственной безопасности).

3. Сочетать при мониторинге как «ручные» способы поиска, так и автоматизированные.

Европейский Союз в рамках инициативы «Европа–2020» определил собственную Цифровую повестку дня (Digital Agenda) с обязательством выполнения широкого круга задач. Первая группа задач повестки ориентирована на дальнейшую популяризацию сети Интернет. Вторая группа задач сводится к обеспечению кибербезопасности граждан. На базе Европейского союза было создано Агентство по сетям и информационной безопасности (ENISA), которое постоянно проводит мониторинг мнений пользователей сети, в соответствии с этим вносит поправки в уже принятые проекты, которые становятся законом и соблюдаются странами ЕС. Отметим, что наиболее важное во всей этой инициативе – то, что законодатели должны проводить ежегодные встречи с политиками, IT-специалистами, учеными для обучения и совершенствования навыков безопасного использования сети Интернет, приучаясь тем самым к виртуальной культуре.

Другой проблемой в сфере безопасности информационных ресурсов является вопрос аттестации объектов информатизации. В соответствии постановлением Кабинета Министров Республики Узбекистан «О совершенствовании нормативно-правовой базы в сфере информатизации» от 22 ноября 2005 г. № 256, Приложение № 2, подпункт 28, примечание 1, обязательной аттестации подлежат: информационная система (ИС) государственного органа и Интернет-ресурс государственного органа. Автор предлагает усовершенствовать мероприятия по обеспечению кибербезопасности следующим образом.

1. Обязать пользователей сети Интернет осуществлять пользование социальными сетями, а также публикацию и комментирование записей и постов только под своими реальными именами.

2. Дополнить действующие Уголовный кодекс и Кодекс об административных правонарушениях Республики Узбекистан составами правонарушений, предусматривающими ответственность за неисполнение или ненадлежащее исполнение обязанностей по обеспечению безопасности государственных информационных систем.

3. Предусмотреть обязательный порядок аттестации объектов информатизации (информационные системы, программное обеспечение) не только для государственных, но и для частных информационных систем.

Подобный подход позволит осуществлять дополнительный контроль за соблюдением банками и субъектами государственного сектора при эксплуатации информационных систем единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

Следует отметить, что одной из значительных мер, предпринятых Республикой Узбекистан в сфере противодействия киберпреступности, явилось включение в новый Уголовный кодекс и Кодекс об административных правонарушениях 2007 г. отдельных глав, посвященных правонарушениям в сфере информационных технологий. Таким образом, можно констатировать систематизацию правоприменительной деятельности в части противодействия правонарушениям в сфере информационных технологий.

LEGAL ISSUES OF CYBERSECURITY STRENGTHENING IN THE REPUBLIC OF UZBEKISTAN

Kh.K. SAMAROV

Abstract. The article deals with the regulatory and legal aspects of strengthening cybersecurity in the Republic of Uzbekistan.

Keywords: information system, information resource, information security, cybersecurity.

Список литературы

1. Безкоровайный М.М., Татузов А.Л. // Вопросы кибербезопасности. 2014. № 1 (2). С. 22–27.
2. Батуева Е.В. // Вестник МГИМО Университета. 2010. №4. С. 271–276.
3. Булавин А.В. // Общество: политика, экономика, право 2014. № 1. С. 27–31.
4. Номоконов В.А., Тропина Т.Л. // Криминология: вчера, сегодня, завтра. 2012. №24. С. 45–55.
5. Погорелова М.А. // Бизнес в законе. Экономико-юридический журнал. 2009. №2. С. 198–200.