НЕКОТОРЫЕ ВОПРОСЫ ЗАКОНОДАТЕЛЬНОГО УКРЕПЛЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

Сабиров К.К.[1], Ахмеджанов Ф.Р.[2]

В свете развития информационных технологий, все большую актуальность обретает проблема законодательного укрепления кибербезопасности. Данный вопрос неоднократно поднимается и главами государств. Так, Президент Казахстана в начале 2017 года поставил задачу разработки национальной системы «Киберщит Казахстана».

Целью статьи является анализ существующих проблемных вопросов в сфере обеспечения кибербезопасности в Республике Казахстан и поиск возможных законодательных путей их решения.

Для этих целей использовался метод сравнительно–правового анализа, с учетом аналогичного опыта Российской Федерации и КНР. В статье были проанализированы наиболее прогрессивные иностранные методики на предмет возможности их имплементации в Республике Казахстан.

В результате нами были выработаны конкретные рекомендации, направленные на правовое закрепление и повышение уровня кибербезопасности в Республике Казахстан. Полученные выводы могут быть использованы, в том числе, и для правового обеспечения разработки системы «Киберщит Казахстана».

***Ключевые слова**: обеспечение кибербезопасности; информационное право; информационная безопасность; уголовное право; защита информации; киберпреступность.*

DOI: 10.21681/2311-3456-2017-3-55-62

На сегодняшний день, в виду 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 правовые и технические механизмы контроля в отношении сетей телекоммуникаций.

Ситуация осложняется тем, что на сегодняшний день активное участие в кибератаках, незаконном сборе информации о чиновниках, корпорациях и простых гражданах принимают государственные структуры развитых стран. При этом применяются и различные методы манипуляция людьми при помощи Интернет-сетей [1, с.23].

Опыт последних лет указывает, что киберпреступность перешагнула границы отдельных государств и стала международной. На актуальность данного вопроса указывает внимание к нему со стороны глав государств. Так, к примеру, в своем послании народу Казахстана от 31 января 2017 года Президент Республики Казахстан Н.А. Назарбаев, поручил Комитету национальной безопасности и Правительству создать систему «Киберщит Казахстана»[3].

Пакет законов РФ о борьбе с терроризмом («пакет Яровой»), принятый летом 2016 года предусматривает, что российские телекоммуникационные и Интернет-провайдеры должны хранить данные пользователей в течение шести месяцев, а метаданные – в течение трех лет. Так же, провайдеры обязаны сотрудничать с властями и передавать все данные для дешифровки.

Во Франции проблемой киберпреступности занимаются с момента принятия Закона Godfrain (Закон № 88-19 от 5 января 1988 года). Юридический арсенал французского законодателя включает в себя: 1. Обязанности операторов и провайдеров сохранять данные не менее года; 2. Возможность привлечь к ответственности любое предприятие и организацию, незаконно обладающую информацией; 3. Возможности прибегнуть к помощи государственных структур, если

1 Сабиров Камал Канаткалиевич, магистр юридических наук; научный сотрудник отдела гражданского, гражданско-процессуального законодательства и исполнительного производства Института законодательства Республики Казахстан. Астана, Республика Казахстаню E-mail: sabirov.k@gmail.com

2 Ахмеджанов Фарух Раушанулы, младший научный сотрудник отдела уголовного, уголовно-процессуального, уголовно-исполнительного законодательства и судебной экспертизы Института законодательства Республики Казахстан. Астана, Республика Казахстан. E-mail: f.akhmedzhanov@adilet.gov.kz

3 См. подробнее: Послание Президента Республики Казахстан Н. Назарбаева народу Казахстана. 31 января 2017 г. // Официальный сайт Президента Республики Казахстан http://www.akorda.kz/ru/addresses/addresses_of_president/poslanie-prezidenta-respubliki-kazahstan-nnazarbaeva-narodu-kazahstana-31-yanvarya-2017-g(Дата обращения: 01.03.2017)

возникала необходимость защиты информации под грифом «секретно» [2].

Лидерство в киберпространстве является и одним из приоритетов США. Курс на усиление информационной безопасности был задан бывшим президентом США Б. Обамой, сразу после его избрания на первый срок. Американская национальная стратегия безопасности строится на дипломатии, разведке, военном комплексе, правоохранительных органах, а также экономических инструментов [3, с.271].

Однако самые эффективные методы защиты информационных данных и обеспечения кибербезопасности существуют в КНР. С 2003 года в Китае 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. Вебстраницы фильтруются по ключевым словам, связанным с государственной безопасностью, а также по «чёрному списку» адресов сайтов. К инструментам работы «Золотого щита» можно отнести: блокировку по IP адресу, DNS, URL, TCP фильтры, блокираторы подключения, создание фальшивых SSL подключений.

Также, согласно Закону КНР «О мерах по регулированию информационных услуг через Интернет» от 1 октября 2000 года- в том случае если провайдер узнает о том, что его сайт содержит информацию представляющую угрозу, он должен сообщить об этом в уполномоченные органы (статья 16). В случае если он этого не делает, то его лицензия может быть отозвана, а деятельность приостановлена (статья 20).

Закон КНР «О кибербезопасности» от 7 ноября 2016 года (далее - Закон КНР 2016 года) предусматривает проведение ежегодных оценок рисков кибербезопасности и предоставление отчётов о результатах этих оценок и мерах по улучшению ситуации соответствующим органам власти (статья 38).

Цель контроля над Интернетом в Китае – предотвратить проникновение нежелательной информации внутрь страны и утечку информации за рубеж, в том числе путем блокирования информационных-ресурсов и поисковых систем [4].

Впрочем, опыт КНР в сфере обеспечения информационной безопасности часто подвергается критике, и является наиболее радикальным. Фактически КНР оградили свою часть глобальной сети «железным занавесом», фильтруя любую информацию, которая как поступает к ним, так и исходит от них.

Следует отметить что, несмотря на законодательное урегулирование в Республике Казахстан 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 Казахстана; уязвимости в отечественных системах защиты информационных ресурсов.

Конвенция Совета Европы о киберпреступности разделила киберпреступность на четыре группы (дополнительный протокол добавил пятую группу). В первую группу были отнесены компьютерные преступления – преступления против конфиденциальности, целостности и доступности компьютерных данных. Во вторую группу входят преступления связанные с использованием компьютерных средств. Третью группу составляют преступления связанные с контентом (содержанием информации в сети). В четвертую группу были отнесены преступления связанные с авторским правом и смежными правами. Наконец пятая группа включает в себя преступления, посягающие на общественную безопасность [5, с.46-47].

На сегодняшний день ряд государств успешно проводит политику укрепления информационной безопасности. В международном опыте можно выделить три основные модели правового регулирования распространения информации в сети Интернет [6, с.198].

Первая модель предусматривает полный контроль государством над сетью Интернет. Данной модели придерживается, к примеру, Китай, где практически весь Интернет находится под полным государственным контролем. Отдельные элементы китайского опыта в настоящее время внедряется в Российской Федерации.

Вторая модель предусматривает ответственность провайдера за любые действия пользователя. Например, во Франции провайдеры обязаны сообщать сведения об авторах сайтов любым заинтересованным третьим лицам. Кроме того, во Франции еще с 1978 года существует специальный орган (Национальная комиссия информатики и свобод), который обязан следить за тем, чтобы информатика не нарушала права и свободы человека.

Третья модель регулирования безопасности в сети Интернет пространства предусматривает освобождение провайдера от ответственности в тех случаях, если он выполняет определенные условия, связанные с характером предоставления услуг и взаимодействия с субъектами информационного обмена. Так, в Германии ответственность провайдеров за размещение нелегального контента на Интернет-ресурсах, находящихся в их сети, наступает лишь в случае, если они сами являются собственником информации, либо сознательно распространяли ее со ссылкой на другие источники. Данная модель также активно используется в Японии.

Отдельные эффективные аспекты опыта данных государств, с учетом отечественной специфики, могут быть реализованы и в Республике Казахстан.

Ключевым вопросом обеспечения информационной безопасности Республики Казахстан является вопрос контроля над хранением и распространением информации. Информация, распространяемая в сетях телекоммуникации, 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 информационных угроз могут находиться вне юрисдикции законодательства Республики Казахстан, что существенно затрудняет применение системы правовых мер.

Во-вторых, в соответствии с подпунктом 2) пункта 1 статьи 15 Закона РК «О связи» операторы связи и (или) владельцы сетей связи, обязаны осуществлять сбор и хранение служебной информации в порядке, определяемом Правительством Республики Казахстан.

Однако закон не предписывает осуществлять сбор и хранение данных пользователей (переписка, звонки и т.д.).

Для сравнения, закон КНР «О мерах по регулированию информационных услуг через Интернет» от 1 октября 2000 года предусматривает, что провайдеры должны хранить такую информацию как время, на которое его подписчики получают выход в Internet, 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 пп. 39 ст. 7 Закона Республики Казахстан «Об информатизации» в компетенцию уполномоченного органа входит содействие собственникам, владельцам и пользователям объектов информатизации 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 Казахстан (пропаганда экстремизма, разжигание межнациональной розни, распространение порнографии и т.п.). Дела рассматриваются в соответствии с ГПК, в частности главами 47 и 48 (особое производство).

Вместе с тем в зарубежных государствах имеется более эффективный опыт блокировки тех или иных Интернет-ресурсов.

Согласно Федеральному закону РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» сайт может быть заблокирован: 1.За призывы к массовым беспорядкам; 2.За призывы к осуществлению экстремистской деятельности; 3.За призывы к участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

При этом указанный закон не обязывает Интернет-провайдера блокировать точечно страницу со спорным текстом, формально провайдер может ограничить доступ по IP-адресу ко всему ресурсу, на котором, наряду с вызвавшей сомнения информацией, размещаются сотни и тысячи других совершенно легитимных материалом.

Также с 2012 года 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 года № 1101.

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

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, к примеру, анализ контента на предмет наличия угроз национальной безопасности отнести к введению органов национальной безопасности и т.д.;

3) сочетать при мониторинге как «ручные» способы поиска так и автоматизированные.

В целом, многие проблемы в сфере обеспечения кибербезопасности становятся возможными вследствие необладания пользователей достаточным уровнем компьютерной грамотности в целях самозащиты.

Существующие в рамках среднего образования дисциплины по изучению основ устройства компьютера и основных компьютерных программ (иначе говоря, «школьная Информатика») являются устаревшими и не соответствуют требованиям времени.

Необходимо смоделировать качественно новые методики изучения данных дисциплин, акцентируя внимание на обучение правилам безопасного поведения в Интернете, а также изучению возможных рисков свободного поведения в сети. В этом случае, уже со школьного возраста будут закладываться основы цифровой грамотности, сопряженные с владением индивидуальными способами защиты от киберугроз.

При этом данная проблема характерна для всей системы кибербезопасности в целом. Можно констатировать полное отсутствие глубокой научной проработки вопросов обеспечения кибербезопасности. Огромное количество нормативно-методических и прочих документов в области защиты информации разработаны в прошлом веке и не учитывают возможные современные каналы утечки информации [7, с.6].

Европейский Союз в рамках инициативы «Европа – 2020» определил собственную Цифровую повестку дня (Digital Agenda) с обязательством выполнения широкого круга задач. Первая группа задач ориентирована на дальнейшую популяризацию Интернета. Вторая группа задач сводится к обеспечению кибербезопасности своих граждан. На базе ЕС 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 проводят ежегодные встречи с политиками, IT-специалистами, учеными для обучения и совершенствования навыков безопасного пользования Интернетом, приучаясь тем самым к виртуальной культуре.

Другим слабым местом доступа в отечественные телекоммуникационные сети является оборудование обеспечивающие функционирование данных сетей. В настоящее время в Республике Казахстан существует процедура сертификации данного оборудования, однако практический анализ показал, что она зачастую проводится формально. Необходимо рассмотреть возможные пути решения указанной проблемы.

В рамках обеспечения безопасности и усиления контроля над телекоммуникационными сетями предлагается рассмотреть опыт других государств.

Так, например, в России согласно федеральному закону РФ «О связи» от 07.07.2003 г. оператор связи, оказывающий услуги по предоставлению доступа к сети «Интернет», обязан обеспечивать установку в своей сети связи, предоставляемых в порядке, предусмотренном федеральным органом исполнительной власти, технических средств контроля за соблюдением оператором связи доступа к сайтам, внесенным в Единый реестр доменных имен, позволяющих идентифицировать сайты, содержащие информацию, распространение которой в Российской Федерации запрещено.

Вместе с тем, Постановлением правительства Республики Казахстан №1593 закрепляется процедура сертификации телекоммуникационного оборудования с функциями ОРМ. Сертификацию осуществляют аккредитованные в установленном порядке юридические лица (п.9). Сертификация осуществляется на соответствие требованиям безопасности, предусмотренным Постановлением №805.

Анализ практики применения подзаконных актов и опыт реализации норм действующего законодательства уполномоченными органами показал, что аккредитованные органы по сертификации проводят испытания зарубежных аппаратных и программных средств формально и не дают гарантий по их безопасности. Как свидетельство, указанные органы за свою деятельность не выявили ни одной «закладки» в зарубежных аппаратных и программных средствах. При этом не имеется гарантия отсутствия в зарубежных аппаратных и программных средствах недокументированных функций - «закладок» (нацеленных на съем информации ограниченного распространения).

Более эффективный опыт сертификации оборудования имеется и в зарубежных странах, в частности в КНР и Российской Федерации.

Согласно Закону КНР 2016 года закупка сетевых продуктов и услуг, которые могут повлиять на национальную безопасность, должна осуществляться под контролем соответствующих органов безопасности (статья 35).

В Российской Федерации также неоднократно поднимали вопрос зависимости гражданской инфраструктуры от иностранного аппаратно-технического обеспечения [8, с.33]. Наконец законодательно с 1 января 2016 года был введен запрет государственным органам закупать иностранные программные обеспечения, кроме случаев, когда в стране нет программного обеспечения с необходимыми функциональными, техническими и (или) эксплуатационными характеристиками[4].

Аналогичные НПА будут актуальны и для Казахстана и будут стимулировать отечественных производителей ПО. На сегодняшний день вся инфраструктура (как государственный, так и частный сектор) построена с использованием зарубежных аппаратных и программных средств. В этой связи, существует прямая зависимость состояния защищенности информационных ресурсов Казахстана от иностранных поставщиков аппаратного и программного обеспечения.

Исследователи отмечают, что в ближайшее время зависимость от иностранных производителей оборудования и разработчиков программного обеспечения может достигнуть критического уровня [9].

Необходимо закрепить законодательное право уполномоченных органов и органов национальной безопасности осуществления проверок оборудования в случае наличия достаточных оснований полагать, что оборудование, используемое оператором связи в обеспечении деятельности телекоммуникационных сетей, представляет угрозу несанкционированного доступа к охраняемой законом информации.

В этой связи целесообразно принятие законодательных мер (разработка государственных программ поддержки) по стимулированию отечественных компаний, производящих продукцию в области защиты информации.

Наконец важным вопросом в сфере обеспечения безопасности Интернет-пространства в Республике Казахстан является вопрос безопасности информационных систем и ресурсов. В настоящее время ввиду популярности иностранных социальных сетей и Интернет-ресурсов и неразвитости отечественных аналогов, существует серьезный пробел в системе безопасности казахстанских информационных систем.

Используемые в настоящее время гражданами Казахстана популярные сервисы социальных сетей (facebook, twitter и т.п.) и мессенджеры (whats up, skype и др.) иностранного производства, что представляет угрозу безопасности информационного пространства при размещении и распространения в них негативного контента. Вместе с тем в силу нахождения доменов иностранных сайтов за рубежом, личные данные пользователей находятся под угрозой незаконного использования со стороны иностранных граждан и спецслужб.

Действующий закон РК «О персональных данных и их защите»[5] предусматривает возможность трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих защиту персональных данных, может осуществляться в случаях (статья 16):

1) наличия согласия субъекта или его законного представителя на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами, ратифицированными РК;

3) предусмотренных законами Республики Казахстан, если это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека и гражданина, здоровья и нравственности населения;

4) защиты конституционных прав и свобод человека и гражданина, если получение согласия субъекта или его законного представителя невозможно.

Данная проблема имеется не только в законодательстве РК. Так, например, в КНР для ее решения в Законе 2016 года обязали сетевых операторов осуществлять хранение личных данных граждан и других важных данных исключительно на территории КНР (статья 37).

Однако включение норм обязывающих операторов хранить информацию на территории Казахстана, может привести к информационной изоляции.

Китайский опыт примечателен еще и тем, что с 2012 года отдельные регионы КНР обязали пользователей сетей выходить в сеть Интернет только под своими реальными именами. А с 2016 года

4 См. Постановление Правительства РФ от 16.11.2015 N 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»

5 См. Закон Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите» // ИПС «Адилет» <http://adilet.zan.kz/rus/docs/Z1300000094> (Дата обращения: 01.03.2017)

данная норма была включена в закон КНР «О кибербезопасности».

Так, власти Пекина объявила, что с 16 марта 2012 года все городские пользователи социальных сетей не указавшие в регистрационных формах своих настоящих имен и фамилий, будут лишены возможности публиковать посты в блогах. Помимо Пекина данные положения были приняты и в ряде других городов КНР – Шанхай, Гуанчжоу, Шэньчжэнь [10].

Закон КНР «О кибербезопасности» 2016 года предусматривает различные обязательства в области защиты безопасности для сетевых операторов, в числе которых верификация подлинности личности пользователей – обязательное требование для определённых сетевых операторов (статья 24).

Актуален и вопрос ответственности лиц, в ведении которых находятся те или иные государственные информационные ресурсы и системы, в частности осуществлении контроля за своевременным принятием мер для обеспечения их защиты.

Другой проблемой в сфере безопасности информационных ресурсов является вопрос аттестации объектов информации. Статья 51 Закона Республики Казахстан «Об информатизации» устанавливает требования об обязательной и необязательной аттестации объектов информатизации[6].

В соответствии с п. 2 обязательной аттестации подлежат:

1) информационная система (ИС) государственного органа;

2) негосударственная ИС, интегрируемая с ИС государственного органа или предназначенная для формирования государственных электронных информационных ресурсов;

3) ИС, отнесенная к критически важным объектам информационно-коммуникационной инфраструктуры;

4) информационно-коммуникационная платформа «электронного правительства»;

5) Интернет-ресурс государственного органа.

В соответствии с п.3 необязательной аттестации подлежат: 1) негосударственная ИС;2) негосударственный Интернет-ресурс.

В качестве предложения, считаем возможным:

1. По опыту китайских коллег обязать пользователей сети Интернет осуществлять пользование социальными сетями, а также публикацию и комментирование записей и постов только под своими реальными именами;

2. Дополнить действующий УК РК и КоАП РК составами правонарушений предусматривающих 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:

- информационных систем дистанционного банковского обслуживания, систем хранения персональных данных клиентов банков, страховых организации.

- информационных систем субъектов квазигосударственного сектора.

Подобный подход позволил бы осуществлять дополнительный контроль за соблюдением банками и субъектами квазигосударственного сектора при эксплуатации данных систем единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, установленных Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

На сегодняшний день мы наблюдаем все признаки институционализации киберпреступности: формируются правовые нормы в борьбе с киберпреступниками, создаются международные институты по кибербезопасности, развиваются новые сферы деятельности, ориентированные на противодействие киберпреступности и др.

В настоящее время в Республике Казахстан существует как техническая, так и правовая база для создания системы безопасности киберпространства и сетей телекоммуникаций.

Следует отметить, что одной из значительных мер, предпринятых Республикой Казахстан в сфере противодействия киберпреступности, явилось включение в новый Уголовный Кодекс и Кодекс об административных правонарушениях 2014 года отдельных глав, посвященных правонарушениям в сфере информатизации и связи. Таким образом, можем констатировать систематизацию деликтного законодательства в части противодействия правонарушениям в сфере информационных технологий. Вместе с тем, отмечаем необходимость реализации подобной меры относительно всей совокупности норм, регулирующих отношения в сфере использования информационно-телекоммуникационных технологий.

6 См. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации» // ИПС «Адилет» < http://adilet.zan.kz/rus/docs/Z1500000418> (Дата обращения: 01.03.2017)

Отмечаем, что на сегодняшний день ни в одной из стран мира нет кодифицированного законодательства по Интернету. Вместе с тем, недостаточность законодательного регулирования сети Интернет в РК представляется явной. В этой связи своевременным было бы принятие отдельного закона «О казахстанском сегменте информационно-телекоммуникационной сети Интернет». Считаем, законопроект, с одной стороны, позволит определить круг дозволенного поведения, а с другой стороны, установить ответственность субъектов сети Интернет, соответствующую современным реалиям и уровню развития общества.

Подобный законопроект уже разрабатывался в РК в 2008 году инициативной группой отечественных юристов. Тогда законопроект не был принят, несмотря на то, что получил существенную поддержку в юридическом сообществе.

Существующие нормативные правовые акты регулируют частные аспекты функционирования сети, прежде всего вопросы подключения к ней через поставщиков, предоставления соответствующих линий связи и т.д. Таким образом, наряду с неотрегулированностью некоторых аспектов функционирования и использования казахстанского сегмента сети Интернет возникают значительные сложности в процессе правоприменения.

Полагаем целесообразным акцентировать внимание на следующем вопросе. Несмотря на то, что большинство граждан и организаций используют услуги связи и передачи данных, предоставляемые крупными сетевыми провайдерами официально и открыто, существует значительное количество организаций, предоставляющих такие услуги анонимно.

В основном к таким организациям относятся иностранные дата-центры, хостинг-компании и Интернет-провайдеры, официально предоставляющие услуги по анонимизации соединения (VPN, Proxy, Socks и др.), а также предоставляющие виртуальный выделенный сервер, оборудование и каналы связи. Отмечаем, что при таких условиях клиенты получают полную анонимность и фактическую безнаказанность в случае использования возможностей анонимности в противоправных целях.

С учетом того, что данные организации выступают в роли информационных посредников, представляется целесообразным закрепить законодательно их ответственность за распространение незаконной информации в сети. Таким образом, данные организации, иначе говоря, сетевые операторы, будут вынуждены обслуживать клиентов, преследующих исключительно законные цели. Данную норму представляется возможным ввести в предложенный ранее законопроект «О казахстанском сегменте информационно-телекоммуникационной сети Интернет».

Полагаем, что затронутые в данной статье проблемы позволяют утверждать, что угрозы кибербезопасности Республики Казахстан в значительной мере исходят из-за пределов РК, что побуждает к ускорению процесса формирования отечественной информационно-телекоммуникационной индустрии.

***Рецензент**: Рахмитов Фуат Марсильевич, кандидат юридических наук, старший научный сотрудник Института законодательства Республики Казахстан.*

Литература:

1. Безкоровайный М.М., Татузов А.Л. Кибербезопасность: подходы к определению понятия // Вопросы кибербезопасности. № 1 (2). 2014. – с.22-27
2. Dechamp C. Cybercriminalite // Defense nationale. – P., 2005. – P. 99-120.
3. Батуева Е.В. Политика администрации Барака Обамы в области обеспечения информационной безопасности // Вестник МГИМО Университета. - №4. 2010. – с.271-276
4. Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика, право, - № 1. – 2014. – с.27-31
5. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. - №24. – 2012. – с.45-55
6. Погорелова М.А. Правовое регулирование распространения информации в сети интернет в условиях глобализации // Бизнес в законе. Экономико-юридический журнал. - №2. – 2009. – С. 198-200.
7. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2) // Вопросы кибербезопасности. №1(2). – 2014. – с.5-12.
8. Севостьянов В.Л. Общественная экспертиза в сфере правового регулирования обеспечения кибербезопасности // Правовая информатика. - №1. 2014. – с. 33-35
9. Згоба А.И., Маркелов Д.В., Смирнов П.И. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. - № 5 (8) . – 2014. – с.30-38
10. Лагуточкин А.В. О проблеме правового регулирования использования сети Интернет в условиях обеспечения безопасности государства // Проблемы правоохранительной деятельности. - №1. – 2012. – С.33-37

SOME ISSUES OF LEGISLATIVE CONSOLIDATION OF CYBERSECURITY IN THE REPUBLIC OF KAZAKHSTAN

K. Sabirov[7], F. Akhmejanov[8]

In the light of the development of the technology, the more and more urgent becomes the issue of the legislative strengthening of cybersecurity. This problem has been even raised by heads of states, for example, the President of Kazakhstan in early of 2017 set the task of developing the system «Cybershield of Kazakhstan».

The aim of the article is to analyze the existing issues in the field of cybersecurity in the Republic of Kazakhstan and the search for possible legislative solutions.

For these purposes, we used comparative legal analysis method, taking into account similar experience of the Russian Federation and China. Article analyzed the most advanced foreign techniques with the possibility of their implementation in the Republic of Kazakhstan.

As a result, article has specific recommendations aimed at the legal consolidation and improvement of cybersecurity in the Republic of Kazakhstan. The conclusions can be used in the development and legal support of the system «Cybershield of Kazakhstan».

Keywords: *Cybersecurity; Informational Law; Informational Security; Criminal law; Data protection; Cybercrime.*

References:

1. Bezkorovajnyj M.M., Tatuzov A.L. Kiberbezopasnost': podhody k opredeleniju ponjatija // Voprosy kiberbezopasnosti. № 1 (2). 2014. – s.22-27
2. Dechamp C. Cybercriminalite // Defense nationale. – P., 2005. – P. 99-120.
3. Batueva E.V. Politika administracii Baraka Obamy v oblasti obespechenija informacionnoj bezopasnosti // Vestnik MGIMO Universiteta. - №4. 2010. – s.271-276
4. Bulavin A.V. O podhodah SShA i Kitaja k obespecheniju kiberbezopasnosti // Obshhestvo: politika, jekonomika, pravo, - № 1. – 2014. – s.27-31
5. Nomokonov V.A., Tropina T.L. Kiberprestupnost' kak novaja kriminal'naja ugroza // Kriminologija: vchera, segodnja, zavtra. - №24. – 2012. – s.45-55
6. Pogorelova M.A. Pravovoe regulirovanie rasprostranenija informacii v seti internet v uslovijah globalizacii // Biznes v zakone. Jekonomiko-juridicheskij zhurnal. - №2. – 2009. – S. 198-200.
7. Borodakij Ju.V., Dobrodeev A.Ju., Butusov I.V. Kiberbezopasnost' kak osnovnoj faktor nacional'noj i mezhdunarodnoj bezopasnosti XXI veka (chast' 2) // Voprosy kiberbezopasnosti. №1(2). – 2014. – s.5-12.
8. Sevost'janov V.L. Obshhestvennaja jekspertiza v sfere pravovogo regulirovanija obespechenija kiberbezopasnosti // Pravovaja informatika. - №1. 2014. – s. 33-35
9. Zgoba A.I., Markelov D.V., Smirnov P.I. Kiberbezopasnost': ugrozy, vyzovy, reshenija // Voprosy kiberbezopasnosti. - № 5 (8) . – 2014. – s.30-38
10. Lagutochkin A.V. O probleme pravovogo regulirovanija ispol'zovanija seti Internet v uslovijah obespechenija bezopasnosti gosudarstva // Problemy pravoohranitel'noj dejatel'nosti. - №1. – 2012. – S.33-37

7 Kamal Sabirov, Master of laws, Researcher of civil, civil procedural legislation and executive proceedings department of the Institute of legislation of the Republic of Kazakhstan. Astana, Republic of Kazakhstan; e-mail: sabirov.k@gmail.com

8 Farukh Akhmejanov, Junior research fellow, department of criminal, criminal procedure, criminal executive legislation and judicial expertise, Institute of legislation of the Republic of Kazakhstan. Astana, Republic of Kazakhstan; e-mail: f.akhmedzhanov@adilet.gov.kz