Network. The Ecological Monitoring and Assessment Network, Coordinating Office and the Canadian Nature Federation, Inquiry Centre Environment Canada, Ottawa, Ontario, 2003. – 24 p.
10. Lefler Tristan E. Successful Community-based Monitoring in Canada: Three Case Studies. University of Guelph, School of Environmental Design and Rural Development, 2010. – 64 p.
11. Quinn Michael S. and Dubois Jennifer E. Community Based Monitoring: Engaging and Empowering. Faculty of Environmental Design, University of Calgary, Calgary, AB, Canada. Alberta Ranchers USDA Forest Service Proceedings RMRS-P-36. 2005. – p. 212-218.
12. Robino Carolina. Community Based Monitoring System. International Development Research Centre, Canada. 2009.8 p.

МЕРЫ ЗАКОНОДАТЕЛЬНОГО УСИЛЕНИЯ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В РАМКАХ ВНЕДРЕНИЯ СИСТЕМЫ «КИБЕРЩИТ КАЗАХСТАНА»

Аннотация. Статья посвящена актуальным вопросам борьбы с киберпреступностью в Республике Казахстан в контексте обеспечения кибербезопасности в свете обозначенных в Послании Президента РК – Лидера Нации Н.А. Назарбаева от 31 января 2017 года «Третья модернизация Казахстана: глобальная конкурентоспособность» приоритетов дальнейшей модернизации.

В статье анализируется действующая в Казахстане правовая база, а также рассмотрен международный опыт в сфере борьбы с киберпреступностью. Вместе с тем, выявлены ключевые вопросы, требующие совершенствования государственного регулирования, в частности: вопросы контроля над сетями телекоммуникаций; вопросы защиты секретной информации, а также личных данных граждан Казахстана; вопросы наличия уязвимостей в отечественных системах защиты информационных ресурсов и программных средствах.

Статья содержит конкретные рекомендации и предложения по итогам анализа проблем правоприменительной практики. Кроме того, тезисы, содержащиеся в работе, могут быть использованы для формирования законодательной базы создания системы «Киберщит Казахстана».
Ключевые слова:противодействие киберпреступности, законодательные меры, безопасность, сеть Интернет, международное сотрудничество.
Аңдатпа. Мақала Қазақстан Республикасының Президенті – Елбасы Н.Ә. Назарбаевтың 2017 жылдың 31 қаңтарындағы «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Жолдауында белгіленген алдағы жаңғырудың негізгі мақсаттарына сай кибер қауіпсіздікті қамтамасыз ету мәнмәтініндегі Қазақстан Республикасының кибер қылмыстылықпен күресуінің өзекті мәселелеріне арналған.

Мақалада Қазақстанда қазіргі уақытта әрекет етуші құқықтық база талданады, сонымен бірге кибер қылмыстылықпен күресу саласындағы халықаралық тәжірибе қарастырылады. Сонымен қатар, мемлекеттік реттеуді жетілдіруді талап ететін басты мәселелер анықталды, мысалы: телекоммуникация торларын бақылау мәселелері; құпия ақпаратты және Қазақстан азаматтарының жеке мәліметтерін қорғау мәселелері; ақпараттық ресурстар мен программалық құралдарды қорғаудың отандық жүйелеріндегі осалдылықтарды анықтау мәселелері.

Мақалада құқық қолдану тәжірибесіндегі мәселелерді талдау нәтижелері бойынша нақты ұсыныстар бар. Одан бөлек, мақала құрамындағы тезистер «Қазақстанның кибер қалқаны» жүйесін құрудың заңнамалық базасын қалыптастыру үшін қолданылуы мүмкін.
Тірек сөздер: кибер қылмыстылыққа қарсы іс-қимыл, заңнамалық шаралар, қауіпсіздік, интернет желісі, халықаралық әріптестік.
Abstract. The article is devoted to topical issues of fighting against cybercrime in the Republic of Kazakhstan in

the context of the further modernization priorities designated in the Message of President of Kazakhstan - Leader of the Nation N.A. Nazarbayev on January 31, 2017 «Third Modernization of Kazakhstan: global competitiveness».

The article analyzes the existing legal framework in Kazakhstan, as well as reviewed the international experience in the fight against cybercrime. At the same time, it identified key issues requiring improvement of government regulation, including: questions of control over telecommunications networks; the protection of classified information and personal data of citizens of Kazakhstan; questions of vulnerabilities in the domestic systems of protection of information resources and software tools.

This article contains specific recommendations and suggestions on the analysis of the problems of law enforcement practice. In addition, theses contained in the paper can be used to form the legal framework creating the system «Cybershield of Kazakhstan».

Keywords: cybercrime, legislation, security, internet, international cooperation

JEL codes*:* K14, K33, K40, K42

АХМЕДЖАНОВ Ф.Р. младший научный сотрудник отдела уголовного, уголовно-процессуального, уголовно-исполнительного законодательства и судебной экспертизы, Институт законодательства Республики Казахстан

САБИРОВ К.К. магистр юридических наук, научный сотрудник отдела гражданского, гражданско-процессуального законодательства и исполнительного производства, Институт законодательства Республики Казахстан

В своем послании народу Казахстана от 31 января 2017 года Президент Республики Казахстан – Лидер Нации Н.А. Назарбаев поручил Комитету национальной безопасности и Правительству создать систему «Киберщит Казахстана» [1]. В условиях количественного и качественного усиления угроз кибербезопасности данная мера является чрезвычайно необходимой.

На сегодняшний день с правовой точки зрения наблюдаются 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. При этом вред, причиненный в результате киберпреступлений, продолжает неуклонно расти.

Киберпреступность способствует нарушению прав, свобод и законных интересов граждан и организаций, а также всерьез угрожает национальной безопасности государства. В этой связи необходимы комплексные меры по созданию эффективной системы противодействия компьютерной преступности. Отмечаем существование ряда сложностей, возникающих при противодействии киберпреступности.

Во-первых, жертвы компьютерной преступности (большинство из них, коммерческие организации) проявляют нежелание сотрудничать с правоохранительными органами, опасаясь распространения мнения о собственной халатности и ненадежной работе своей фирмы.

Во-вторых, источники информационных угроз могут находиться вне юрисдикции законодательства Республики Казахстан, что существенно затрудняет применение системы правовых мер.

В-третьих, актуальной проблемой является отсутствие отечественных информационных технологий, что вынуждает массового потребителя приобретать импортную технику, не имеющую подтверждения соответствия требованиям информационной безопасности. Данное положение способствует зависимости государства от иностранных производителей

компьютерной, телекоммуникационной техники и информационной продукции.

В-четвертых, отмечается бессистемность защиты данных и слабая координация мер по защите информации в общегосударственном масштабе, ведомственная разобщенность в обеспечении целостности и конфиденциальности информации.

Отметим, что в настоящее время в Республике Казахстан создана и функционирует как техническая, так и правовая база для создания системы безопасности киберпространства и сетей телекоммуникаций.

Одной из значительных мер, предпринятых Республикой Казахстан в сфере противодействия киберпреступности, явилось включение в Уголовный Кодекс и Кодекс об административных правонарушениях 2014 года отдельных глав, посвященных правонарушениям в сфере информатизации и связи. Так, глава 7 включает девять статей, среди которых уголовная ответственность предусматривается за неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций; создание, использование или распространение вредоносных компьютерных программ и программных продуктов и др. В соответствии со ст. ст. 187, 191 УПК РК досудебное расследование по уголовным правонарушениям названной главы осуществляется органами внутренних дел и органами национальной безопасности.

Таким образом, можем констатировать упорядоченность деликтного законодательства в части противодействия правонарушениям в сфере информационных технологий. Вместе с тем, отмечаем необходимость реализации подобной меры относительно всей совокупности норм, регулирующих общественные отношения в сфере использования информационно-телекоммуникационных технологий.

Несмотря на законодательное урегулирование в Республике Казахстан вопроса обеспечения кибербезопасности, эффективному процессу построения системы защиты информационного пространства препятствует ряд проблемных вопросов, требующих государственного регулирования. 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; вопросы наличия уязвимостей в отечественных системах защиты информационных ресурсов и программных средствах.

Как отмечалось, в числе прочих возникают проблемы, связанные с обеспечением государственного контроля над телекоммуникационными сетями. Представляется, что в условиях присутствия активной угрозы нарушения прав и свобод граждан и организаций государству необходимо постоянно совершенствовать правовые и технические механизмы контроля в отношении сетей телекоммуникаций.

Следует отметить, что сегодня ряд государств достаточно успешно осуществляет политику укрепления информационной безопасности. Опираясь на международный опыт, можно выделить три основные модели правового регулирования распространения информации в сети Интернет [2].

Первая модель предусматривает установление полного государственного контроля над сетью Интернет. Данной модели придерживается, к примеру, Китай, где практически весь Интернет находится под полным государственным контролем. Заметим, что отдельные элементы китайской модели в настоящее время внедряются и 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 противозаконного материала 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.

Полагаем, что необходим глубокий анализ указанных моделей в целях выявления их недостатков и наиболее эффективных элементов на предмет возможности дальнейшей имплементацией в казахстанское законодательство.

Ключевым блоком вопросов в данной статье мы определяем вопросы оперативно-розыскной и уголовно-процессуальной деятельности по укреплению кибербезопасности в сферах хранения и распространения информации, создания и функционирования телекоммуникационных сетей, обеспечения безопасности информационных систем и информационных ресурсов.

На сегодняшний день законодательство Республики Казахстан предусматривает возможность получения доступа к информации на сетях телекоммуникаций по запросу правоохранительных органов. Данные действия осуществляются в соответствии с положениями Уголовно-процессуального кодекса РК, Закона РК «Об оперативно-розыскной деятельности», а также ведомственных нормативных правовых актов.

Вместе с тем, доступ не всегда предоставляется в достаточной для проведения оперативно-розыскных мероприятий степени. Проведенный анализ законодательства указал на возможные пути совершенствования правовой базы в рамках укрепления кибербезопасности в сфере оперативно-розыскной деятельности.

Подпункт 6) Закона «Об оперативно-розыскной деятельности» *(далее - Закон)* содержит понятие «оперативный поиск на сетях связи», под которым понимаются «негласные действия по обнаружению признаков противоправной деятельности в информации, передаваемой по сети связи». Вместе с тем, субъекты оперативно розыскной деятельности *(далее – ОРД)* могут осуществлять и иные оперативно-розыскные мероприятия *(далее – ОРМ)*, сопряженные с использованием технических средств связи [3].

Согласно подпункту а) статьи 7 Закона, органы ОРД обязаны «принимать в соответствии с компетенцией необходимые меры для защиты охраняемых законом прав, свобод и интересов физических и юридических лиц, собственности, безопасности общества, государства и укрепления его экономического и оборонного потенциала». Данное обязательство вытекает из конституционного положения о необходимости защиты государством прав, свобод и законных интересов каждого.

Таким образом, в случае наличия угрозы несанкционированного доступа к охраняемой законом информации, либо угрозы распространения информации, содержащей противоправные цели, субъекты ОРД обязаны принимать соответствующие меры по предупреждению указанных угроз.

Отмечаем, что сети телекоммуникаций выступают ключевым звеном в системе обеспечения информационной безопасности государства. В целях обеспечения деятельности субъектов ОРД по проведению ОРМ на сетях телекоммуникаций разработаны и утверждены:

- Постановление Правительства РК от 31 января 2001 года №164 «Об утверждении Правил подготовки и использования сетей телекоммуникаций общего пользования, ресурсов единой сети телекоммуникаций для нужд государственных органов, органов

обороны, безопасности и охраны правопорядка Республики Казахстан»;

- Постановление Правительства РК от 23 декабря 2011 года №1593 «Об утверждении Правил взаимодействия органов, осуществляющих оперативно-розыскные мероприятия, и организаций при внедрении и эксплуатации аппаратно-программных и технических средств проведения оперативно-розыскных мероприятий на сетях телекоммуникаций Республики Казахстан»;

- Постановление Правительства РК от 6 августа 2010 года №805 «Об утверждении технического регламента «Общие требования безопасности, функциональные и технические требования к телекоммуникационному оборудованию при проведении оперативно-розыскных мероприятий» и др.

Согласно пункту 2 Постановления Правительства Республики Казахстан от 31 января 2001 года № 164 «под взаимоувязанной сетью телекоммуникаций понимается комплекс технологически сопряженных сетей телекоммуникаций на территории Республики Казахстан, обеспеченный централизованным управлением». «Сеть телекоммуникаций общего пользования – составная часть взаимоувязанной сети телекоммуникаций, открытая для пользования всем физическим и юридическим лицам» [4].

В этом же постановлении указано, что операторы связи, действующие на территории РК, независимо от форм собственности и ведомственной принадлежности обязаны в соответствии с Законами РК «О связи» и «Об оперативно-розыскной деятельности» обеспечивать органам, осуществляющим оперативно розыскную деятельность, организационные и технические возможности проведения оперативно-розыскных мероприятий на всех сетях связи, принимать меры по недопущению раскрытия форм и методов проведения указанных мероприятий (п.19).

Таким образом, отмечаем, что для целей ОРД не имеет значения форма собственности оператора связи или владельца сети телекоммуникаций. При наличии достаточных оснований и соблюдении предусмотренных законом процедур организации обязаны оказывать содействие субъектам ОРД в той мере, в которой это потребуется в целях защиты охраняемых прав и свобод, законных интересов.

Для дополнительного закрепления гарантий правоохранительной деятельности в сфере противодействия киберпреступности целесообразно в Законе РК «О связи» указать, что при наличии достаточных оснований и соблюдении предусмотренных законом процедур организации обязаны оказывать содействие субъектам ОРД в необходимой мере.

Вместе с тем, учитывая специфику процесса расследования киберпреступлений, предлагаем: 1) провести анализ практики расследования данной категории преступлений с целью выявления недостатков в действующем оперативно-розыскном и уголовно-процессуальном законодательстве для дальнейшего его совершенствования; 2) изучить вопрос материальной и кадровой оснащенности органов досудебного расследования с целью дальнейшего принятия мер для их «дооснащения» с учетом актуальных тенденций и угроз.

В числе киберпреступлений одним из наиболее распространенных видов является так называемый «компьютерный фишинг». При этом киберпреступниками используется «продвинутое» программное обеспечение, которое позволяет удаленно управлять компьютерами без ведома их пользователей. Их называют ботами, а сеть компьютеров, зараженных вредоносным кодом, – ботнетами. Необходимо отметить, что подавляющая часть обычных пользователей остаются беззащитной перед лицом указанных угроз и не в состоянии противостоять профессиональным действиям киберпреступников.

Подобные преступления направлены на получение незаконного доступа к конфиденциальным данным пользователей и их дальнейшее использование. Следует

отметить, что данная ситуация становится возможной вследствие необладания пользователями достаточным уровнем компьютерной грамотности в целях самозащиты. Существующие в Республике Казахстан 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.

В этой связи, полагаем необходимым в качестве одной из мер противодействия киберпреступности на постоянной основе повышать компьютерную грамотность населения, преимущественно молодежи. Необходимо смоделировать качественно новые методики изучения указанных дисциплин, акцентируя внимание на обучении правилам безопасного поведения в сети Интернет, 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.

Ранее отмечалось, что уязвимость перед киберпреступниками создается посредством использования небезопасного программного оборудования. На сегодняшний день в Казахстане вся инфраструктура (как государственный, так и частный сектор) построена с использованием зарубежных аппаратных и программных средств. Касательно этого вопроса справедливо отмечено в Концепции информационной безопасности Республики Казахстан до 2016 года: «Отсутствие соответствующих потребностям государства, бизнеса и общества отечественных информационных технологий приводит к вынужденному использованию иностранного оборудования и информационных систем. В результате этого повышается вероятность несанкционированного доступа к базам и банкам данных, а также возрастает зависимость страны от иностранных производителей компьютерной и телекоммуникационной техники и программного обеспечения» [5]. В частности, вся сетевая инфраструктура Казахстана построена с использованием сетевого оборудования китайского и американского производства.

Вместе с тем, Постановлением Правительства Республики Казахстан от 23 декабря 2011 года №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 Правительства РК от 6 августа 2010 года №805 [6].

Несмотря на это, аккредитованные органы по сертификации проводят испытания зарубежных аппаратных и программных средств формально, не предоставляя гарантий по их безопасности. В этой связи, необходимо законодательно ужесточить порядок контроля проведения сертификации телекоммуникационного оборудования.

Кроме того, необходимо закрепить законодательное право уполномоченных органов и органов национальной безопасности осуществления проверок телекоммуникационного 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 либо может быть использовано в целях совершения иных киберпреступлений.

В целях повышения конкурентноспособности отечественной информационной продукции требуется принятие законодательных мер (разработка государственных программ поддержки) по стимулированию отечественных компаний, производящих продукцию в области защиты информации.

Для повышения эффективности, упрощения процедуры и оперативного принятия мер по пресечению распространения незаконного контента предлагается упростить существующую процедуру блокировки Интернет-ресурсов посредством предоставления права уполномоченному органу самостоятельной блокировки без обращения в суд. В дальнейшем законность и обоснованность данной меры должна быть подтверждена.

Представляется, что может быть полезен российский опыт ведения единого реестра запрещенных сайтов. При этом возможно распределить функции мониторинга Интернет пространства между некоторыми государственными органами, к примеру, анализ контента на предмет наличия угроз национальной безопасности отнести к компетенции органов национальной безопасности и т.д. При осуществлении мониторинга необходимо сочетать как «ручные» способы поиска, так и автоматизированные.

Считаем целесообразным проведение уполномоченными правоохранительными органами в сфере противодействия киберпреступности мониторинга мнений пользователей телекоммуникационных сетей на предмет выявления актуальных угроз кибербезопасности. Данная мера может быть реализована посредством размещения соответствующих опросов в средствах массовой информации, а также на популярных Интернет-порталах, в том числе на ведомственных сайтах.

Кроме этого, необходимо проработать вопрос о закреплении в законодательстве обязанности операторов и владельцев сетей телекоммуникаций по осуществлению мониторинга информационного пространства и сообщению о сайтах, потенциально угрожающих безопасности. Вместе тем, интересен китайский опыт по периодическому обобщению практики обеспечения информационной безопасности, включая оценку рисков кибербезопасности и их нивелирования.

Уязвимым также является механизм сбора, хранения и обеспечения конфиденциальности персональных данных пользователей. Отмечаем, что эти уязвимости наиболее часто используются для совершения киберпреступлений. Поэтому, учитывая важность направления борьбы не только с киберпреступностью, но и с терроризмом и экстремизмом, полагаем целесообразным рассмотреть возможность осуществления сбора и хранения данных пользователей по аналогии с российским и китайским опытом (Закон «Яровой» и др.).

В настоящее время в Республике Казахстан созданы и функционируют специальные правоохранительные подразделения по борьбе с киберпреступностью: Служба по борьбе с киберпреступлениями в структуре КНБ РК, а также Управление «К» в структуре МВД РК. Таким образом, вопрос создания отдельного уполномоченного органа не ставится. Вместе с тем представляется, что для повышения эффективности борьбы с киберпреступностью необходимо постоянное повышение профессиональной компетенции сотрудников указанных подразделений.

В этих целях предлагаем создать механизм прохождения указанными сотрудниками на систематической основе курсов повышения квалификации в ведущих информационно-технических центрах мира, в том числе крупных IT-компаниях (Microsoft, Google, Лаборатория Касперского). На сегодняшний день повышение квалификации осуществляется путем проведения тренингов, семинаров, а также гостевых лекций. Данные меры не способны в необходимой степени повысить конкурентоспособность отечественных правоохранителей. Важность взаимодействия с IT-центрами заключается в том, что именно они зачастую первыми выявляют вновь создаваемые киберпреступниками угрозы, а также методы их обнаружения и борьбы с ними.

Кроме того, необходимо по аналогии с российским опытом обеспечить обширную систему информирования пользователей о

возможных угрозах, стандартных уловках преступников, а также мерах, позволяющих минимизировать риски при работе в киберпространстве. Данная информация может быть распространена как в бумажном (выпуск брошюр), так и в электронном виде (рассылки сообщений).

Поднимаемые в рамках данного исследования проблемы, а также важность их незамедлительного решения порождают необходимость в упорядочивании общественных отношений в сфере осуществления государством мер противодействия киберпреступности.

В целях реализации поручения Главы государства по разработке системы «Киберщит Казахстана» возникает необходимость принятия отдельного законодательного акта «О противодействии киберпреступности» аналогично существующим законодательным актам о противодействии терроризму и экстремизму, что позволило бы создать специальную правовую базу для функционирования системы «Киберщит Казахстана».

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 [7, с. 44]. 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 полагаем целесообразным ввести в предложенный ранее законопроект «О противодействии киберпреступности».

Учитывая транснациональный характер современной киберпреступности, считаем необходимым проработать вопрос укрепления международного сотрудничества Казахстана в этой области. В частности, выявить наиболее перспективные направления и цели. Полагаем, что в условиях ускоренного развития информатизации казахстанского общества, а также с учетом обострившейся угрозы международного терроризма и участившихся профессионально подготовленных акций со стороны киберпреступников работа в данном направлении своевременна.

Нельзя не отметить имеющиеся международно-правовые документы в области борьбы с киберпреступностью. Так, единственным признанным на сегодняшний день подобным документом является Конвенция Совета Европы от 23 ноября 2001 года о компьютерных преступлениях. Конвенция направлена на укрепление взаимного сотрудничества государств-членов в области обеспечения кибербезопасности, а также обмена информацией, обеспечения доступа к информационным ресурсам в целях пресечения преступлений.

Конвенция также требует создать необходимые правовые условия, в частности, обязать Интернет-провайдеров проводить сбор и фиксацию или перехват необходимой информации с помощью имеющихся технических средств, а также способствовать в этом правоохранительным органам. При этом рекомендуется обязать провайдеров сохранять полную конфиденциальность о фактах подобного сотрудничества [8].

В документе подробно описаны проблемы взаимодействия

правоохранительных органов отдельных государств в ситуациях, когда преступник и жертва находятся в разных странах и подчиняются различным законодательствам. Конвенция также оговаривает общие для всех интернет-провайдеров правила хранения личной информации клиентов на случай, если подобные сведения будут затребованы при расследовании киберпреступлений [9].

Считаем возможным проанализировать конвенцию Совета Европы на предмет возможных рисков и угроз национальной безопасности и последующего присоединения к ней с оговорками.

Вместе с тем, транснациональный характер современной киберпреступности и в этой связи необходимость укрепления межгосударственного сотрудничества в области борьбы с киберпреступностью ставит вопрос о создании межгосударственного органа по борьбе с киберпреступностью на уровне СНГ или других региональных объединений. Данный орган может показать свою эффективность, так как будет сформирован из сотрудников правоохранительных органов, будет действовать на основании международного договора, а также пользоваться экстерриториальностью.

В качестве справки, компания Microsoft 19 ноября 2013 года открыла Центр по борьбе с мировой киберпреступностью. Центр открыт в штаб-квартире корпорации в Редмонде, штат Вашингтон, США. Его подразделения будут функционировать еще в 12 офисах и региональных лабораториях компании по всему миру: в Пекине, Берлине, Боготе, Брюсселе, Дублине, Эдинборо (США), Гургаоне (Индия), Гонконге, Мюнхене, Сингапуре, Сиднее и Вашингтоне. В Центре работает почти 100 адвокатов, следователей, технических экспертов и судебных аналитиков со всего мира. Основные направления работы сотрудников Центра по борьбе с мировой киберпреступностью: борьба с бот-сетями; розыск украденной техники по следам, оставляемым в сети Интернет; противодействие распространению пиратских, некачественных программных продуктов под брендами известных IT-компаний [10].

Полагаем, что затронутые в данном исследовании 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. На данном же этапе ее развития в качестве альтернативного пути предупреждения киберугроз иностранного происхождения необходимо обеспечить контроль над всеми финансовыми операциями на территории РК, связанными с деятельностью иностранных телекоммуникационных сетей, их собственников, провайдеров и операторов связи.

Зарубежное финансирование с точки зрения угроз кибербезопасности может быть направлено на разработку и обеспечение различного рода подрывных акций, включая хакерские атаки, внедрение программного обеспечения с уязвимостями и др. В этой связи, отслеживание процедуры расходования средств, поступивших из-за рубежа, представляется крайне необходимым. Отметим, что ставить вопрос о запрете иностранного финансирования (по аналогии с конституционным положением о запрете иностранного финансирования политических партий и профессиональных союзов (пункт 4 статьи 5 Конституции РК)) на данном этапе нецелесообразно в силу неразвитости отечественного рынка.

Опираясь на изложенный в данной статье материал, отмечаем, что концепция создания эффективной системы кибербезопасности основывается на следующем тезисе: государство должно обеспечить контроль над входом информации в страну, ее выходом за пределы страны, а также над движением информации внутри страны. При этом основанная на данном принципе система не должна ограничивать конституционные права и свободы человека.

Список литературы

1.Послание Президента Республики Казахстан Н.А. Назарбаева народу Казахстана от 31 января 2017 года «Третья модернизация Казахстана: глобальная конкурентоспособность» // Официальный сайт Президента Республики Казахстан [Электронный ресурс]. – Режим доступа: http://www.akorda.kz/ru/addresses/ addresses_of_president/poslanie-prezidenta-respubliki-kazahstan-nnazarbaeva-narodu-kazahstana-31-yanvarya-2017-g;
2. Погорелова М.А. Правовое регулирование распространения информации в сети интернет в условиях глобализации // Бизнес в законе. Экономико-юридический журнал. - № 2. – 2009. – С. 198-200;
3. Закон Республики Казахстан от 15 сентября 1994 года № 154-XIII «Об оперативно-розыскной деятельности» (по состоянию на 02.03.2017) // ИПС «Аділет» [Электронный ресурс]. – Режим доступа: http://adilet.zan.kz/rus/docs/Z940004000_;
4. Постановление Правительства Республики Казахстан от 31 января 2001 года № 164 «Об утверждении Правил подготовки и использования сетей телекоммуникаций общего пользования, ресурсов единой сети телекоммуникаций для нужд государственных органов, органов обороны, безопасности и охраны правопорядка Республики Казахстан» (по состоянию на 02.03.2017) // ИПС «Аділет» [Электронный ресурс]. – Режим доступа: http://adilet.zan.kz/rus/docs/P010000164;
5.Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года» // ИПС «Аділет» [Электронный ресурс]. – Режим доступа: http://adilet.zan.kz/rus/docs/U1100000174;
6. Постановление Правительства Республики Казахстан от 23 декабря 2011 года № 1593 «Об утверждении Правил взаимодействия органов, осуществляющих оперативно-розыскные мероприятия, и организаций при внедрении и эксплуатации аппаратно-программных и технических средств проведения оперативно-розыскных мероприятий на сетях телекоммуникаций Республики Казахстан» (по состоянию на 02.03.2017) // ИПС «Аділет» [Электронный ресурс]. – Режим доступа: http://adilet.zan.kz/rus/docs/P1100001593;
7. Галушкин А.А. К вопросу о кибертерроризме и киберпреступности // Журнал Вестник Российского университета дружбы народов. Серия: Юридические науки. Выпуск № 2 / 2014. – С. 44-49;
8. Преступления в сфере информационных технологий // Сайт «Академик» [Электронный ресурс]. – Режим доступа: http://dic.academic.ru/dic.nsf/ruwiki/1328051;
9. Юридическая ответственность за киберпреступления в России. Взгляд России на международные решения по борьбе с компьютерными преступлениями. // Сайт «Zakon.ru» [Электронный ресурс]. – Режим доступа: https://zakon.ru/blog/2012/1/15/yuridicheskaya_otvetstvennost_za_kiberprestupleniya_v_rossii_vzglyad_rossii_na_mezhdunarodnye_reshen;
10. Microsoft открыла современный Центр по борьбе с киберпреступностью // Сайт компании Microsoft [Электронный ресурс]. – Режим доступа: https://news.microsoft.com/ru-ru/microsoft-otkry-la-sovremenny-j-tsentr-po-bor-be/#sm.0000anhejy13oxcy1qxl6ok88jcnn#P7DGsGOizmA5YcpM.97.