УДК 004.056(597) Вестник УрФО № 1(31) / 2019, с. 64–68

Минбалеев А. В.

DOI: 10.14529/secur190110

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ВО ВЬЕТНАМЕ[1]

В статье автор описывает систему кибербезопасности во Вьетнаме. Комплексные нормативные правовые акты, посвященные вопросам кибербезопасности, стали приниматься в мире на волне стремительно увеличивающегося числа вызовов и угроз в информационной сфере. Одним из первых таких законов стали законы о кибербезопасности в Китае и во Вьетнаме. Принятие закона во Вьетнаме встретило очень серьезную критику со стороны ряда других стран и международных организаций. Ключевые слова: право на информацию, право на достоверную информацию, информация, информационное общество, общество знаний. Закон о кибербезопасности предусматривает защиту национальной безопасности и поддержание общественного порядка и безопасности в киберпространстве, а также закрепляет ряд соответствующих обязанностей органов власти, организаций и отдельных лиц. В статье анализируются основные понятия закона о кибербезопасности, приницпы регулирования и механизмы регулирования отношений в сфере обеспечения кибербезопасности.

Ключевые слова: *кибербезопасность, информационная безопасность, правовое регулирование, Вьетнам.*

Minbaleev A. V.

LEGAL ENSURING OF CYBER SECURITY IN VIETNAM

In the article the author describes the system of cybersecurity in Vietnam. Complex normative legal acts devoted to cybersecurity issues have been adopted in the world in the Wake of the rapidly increasing number of challenges and threats in the information sphere. One of the first such laws was the law on cybersecurity in China and Vietnam. The adoption of the law in Vietnam has met with very serious criticism from a number of other countries and international organizations. Keywords: right to information, right to reliable information, information, information society, knowledge society. The law on cybersecurity provides for the protection of national security and the maintenance of public order and security in cyberspace, as well as establishes a number of relevant responsibilities of authorities, organizations and individuals.the article analyzes the basic concepts of the law on cybersecurity, the principles of regulation and mechanisms of regulation of relations in the field of cybersecurity.

Keywords: *cybersecurity, information security, legal regulation, Vietnam.*

[1] Статья написана в рамках Государственного задания по теме «Правовое регулирование цифровой экономики, искусственного интеллекта информационной безопасности».

Обеспечение кибербезопасности сегодня становится одной из ключевых задач современного государства в рамках общей системы обеспечения государством информационной безопасности. Правовое обеспечение информационной безопасности в последние годы связывается с целой системой новых по своему характеру нормативных правовых актов. Если ранее в основном это были акты, регулирующие вопросы информации ограниченного доступа, противодействия компьютерной преступности, лицензирования и сертификации защиты информации, то сегодня появляются законы и стратегические акты, посвященные вопросам кибербезопасности, киберугроз, противодействия использования информационного оружия.

Комплексные нормативные правовые акты, посвященные вопросам кибербезопасности, стали приниматься в мире на волне стремительно увеличивающегося числа вызовов и угроз в информационной сфере. Одним из первых таких законов стали законы о кибербезопасности в Китае и во Вьетнаме.

Принятие закона во Вьетнаме встретило очень серьезную критику со стороны ряда других стран и международных организаций. Соединенные Штаты и Канада настоятельно призвали Вьетнам отложить голосование по законопроекту, чтобы он соответствовал международным нормам. Так, в заявлении посольства США во Вьетнаме отмечалось, что «законопроект о кибербезопасности может привести к серьезным препятствиям для будущего кибербезопасности и технических инноваций, может не соответствовать международным обязательствам Вьетнама по международной торговле» [1]

В качестве основных замечаний оппозиции выступили опасения, что принятие закона серьезно ограничит развитие цифровой экономики и инвестиционного климата. По данным Ассоциации цифровых СМИ Вьетнама, закон может снизить рост ВВП на 1,7% и сократить иностранные инвестиции на 3,1% во Вьетнаме. По оценкам, около 70 % из 93 миллионов человек во Вьетнаме имеют доступ в Интернет, а около 53 миллионов имеют учетные записи Facebook. Джефф Пейн, исполнительный директор Азиатского интернет-альянса (отраслевая ассоциация, включая Google и Facebook) отметил, что они «разочарованы» принятием законодательства, которое потребует внутренних геокодирование, управление контентом и локализацию. Глобальные технологические компании особо выразили свое несогласие с правилами о местном хранении пользовательских данных. Делегат Национальной ассамблеи Нгуен Тхи Ким Туй отметил, что Закон о кибербезопасности может противоречить обязательствам Вьетнама в рамках ВТО и Соглашению о свободной торговле между ЕС и Вьетнамом [2].

Необходимо отдать должное вьетнамским властям, что, несмотря на сильное лоббирование недопущения принятия закона, он был ратифицирован членами Национального собрания Вьетнама. Как отметила пресс-секретарь МИД Вьетнам Ле Тхи Ту Хан, «валидация закона о кибербезопасности заключается в создании безопасного и здорового киберпространства…это защитит законные права и интересы организаций и частных лиц в Интернете, а также обеспечит национальную безопасность, а также социальный порядок и безопасность. Вьетнамское государство всегда уважает и дает людям возможность практиковать свои права и свободы, но решительно защищает от злоупотребления этими правами для осуществления незаконной деятельности» [3].

Закон о кибербезопасности предусматривает защиту национальной безопасности и поддержание общественного порядка и безопасности в киберпространстве, а также закрепляет ряд соответствующих обязанностей органов власти, организаций и отдельных лиц. При этом под киберпростарнством в целом понимается сеть инфраструктуры информационных технологий, включая телекоммуникационные сети, Интернет, компьютерные сети, информационные системы, системы обработки информации и управления данными; место, неограниченное пространством и временем, где люди осуществляют социальное поведение. Под национальным киберпространством понимается киберпространство, созданное, управляемое и контролируемое правительством (соответственно правительством Вьетнама). Таким образом, киберпространство прямо признается законодателем не как чисто техническая система, а социотехническая система, в которой осуществляется социальное поведение, подпадающее под действие ряда социальных регуляторов.

Национальная киберинфраструктура представляет собой систему средств и технологий для создания, передачи, сбора, обра-

ботки, хранения и обмена информацией о национальном киберпространстве, в том числе:

– система передачи данных, состоящая из национальной системы передачи данных, международной системы передачи данных, спутниковой системы, системы оказания услуг поставщиками по сетям электросвязи, в том числе телекоммуникационной сети Интернет, и услугах, направленных на расширение использования киберпространства;

– система основных услуг, включающая в себя национальную систему передачи информации и навигации, национальную систему распределения доменных имен (DNS), национальную систему аутентификации (PKI / CA) и систему поставок услуг связи, телекоммуникационных услуг в сети Интернет, интернет-сервисы;

– услуги и приложения в области информационных технологий, включая онлайн-сервисы; применение информационных технологий с сетевым подключением для управления и администрирования важных экономических и финансовых агентств, организаций и корпораций; Национальная база данных.

– онлайн-сервисы, включающие электронное правительство, электронную коммерцию, веб-сайты, онлайн-форумы, социальные сети, блоги;

– инфраструктура информационных технологий умного города, универсальный Интернет, система виртуальной реальности, облачные вычисления, система больших данных, системы мгновенной передачи данных и интеллектуальные системы.

Кибербезопасность (сетевая безопасность), согласно анализируемому Закону о кибербезопасности, означает гарантию (обеспечение) функционирования в киберпространстве без ущерба для национальной безопасности, социального порядка и безопасности, законных прав и интересов органов власти, организаций и отдельных лиц. Под угрозами кибербезопасности рассматриваются любые ситуации, при которых киберпространство угрожает нарушить национальную безопасность, нанося серьезный ущерб социальному порядку, безопасности, законным правам и интересам органам власти, организациям и частным лицам. Угрозы при этом связываются с инцидентами кибербезопасности и опасными ситуациями кибербезопасности. Под инцидентами кибербезопасности понимаются неожиданные инциденты в киберпространстве, затрагивающие национальную безопасность, социальный порядок и безопасность, законные права и интересы органов власти, организаций и частных лиц. Опасные ситуации кибербезопасности означают инциденты в киберпространстве, при которых происходит серьезное нарушение национальной безопасности, особенно серьезный ущерб социальному порядку, безопасности, правам и охраняемым законом интересам органов власти, организаций и частных лиц.

Закон определяет основные понятия, связанные с киберпреступностью как актом использования киберпространства, информационных технологий или электронных средств для совершения преступлений, предусмотренных Уголовным кодексом. Под киберперступностью понимаются любые преступления, которые совершаются с использованием киберпространства, информационных технологий или электронных средств. Под кибератаками понимаются акты использования киберпространства, информационных технологий или электронных средств для саботажа, нарушения работы телекоммуникационных сетей, в том числе сети Интернета, компьютерных сетей, информационных систем и систем обработки и управления информацией, базами данных и электронными средствами.

Отдельно вводятся понятия сетевого терроризма как использования киберпространства, информационных технологий или электронных средств для осуществления террористических актов и финансирования терроризма, а также сетевого шпионажа как акта преднамеренного преодоления предупреждений, кодов доступа, паролей, межсетевых экранов, использования административных прав других лиц или других способов присвоения, незаконного сбора информации, информационных ресурсов через телекоммуникационные сети, в том числе сети Интернет, компьютерным сетям, информационным системам, системам обработки и управления информацией, базам данных и электронным средствам органов власти, организаций и частных лиц. Цифровая учетная запись означает информацию, используемую для аутентификации, аутентификации, децентрализации использования приложений и услуг в киберпространстве.

Законодатель устанавливает ряд принципов защиты кибербезопасности, то есть предупреждения, обнаружения, предотвращения

и устранение нарушений кибербезопасности:

– законность; обеспечение интересов государства, законных прав и интересов органов власти, организаций и отдельных лиц;

– обеспечение единого управления государством под руководством Коммунистической партии Вьетнама; мобилизация объединенной власти политической системы и всей нации; продвижение основной роли сил защиты сети;

– тесное сочетание задачи защиты сетевой безопасности, защиты важной информационной системы национальной безопасности с задачей социально-экономического развития, обеспечения прав человека и гражданина, создания условий для функционирования органов власти, организаций и частных лиц в киберпространстве.

– предупреждение, обнаружение, предотвращение, борьба и отказ от всех видов деятельности, связанной с использованием киберпространства с целью нарушения национальной безопасности, общественного порядка и безопасности, законных прав и интересов органов власти, юридических и физических лиц; оперативность предотвращения киберугроз;

– реализация защиты кибербезопасности для национальной инфраструктуры киберпространства; применение мер по защите важных информационных систем в области национальной безопасности.

– необходимость аудита и сертификации значимых информационных систем в области национальной безопасности на предмет кибербезопасности перед вводом в эксплуатацию и использованием; регулярность проверки и контроля безопасности сети в процессе использования и оперативного реагирования, устранения неполадок, связанных с кибербезопасностью.

– все действия, нарушающие закон о кибербезопасности, должны решаться быстро и строго.

Закона о кибербезопасности устанавливает и ряд мер по обеспечению кибербезопасности: оценка кибербезопасности; оценка состояния кибербезопасности ; мониторинг кибербезопасности; реагирование и устранение неполадок в сфере кибербезопасности; борьба за обеспечение кибербезопасности; использование паролей для защиты сетевой информации; предотвращение предоставления, приостановление или прекращение предоставления сетевой информации; предупреждение, приостановление деятельности по созданию, обслуживанию и использованию телекоммуникационных сетей, сети Интернет; запрос на удаление незаконной информации или ложной информации в киберпространстве, распространенной с целью нарушения национальной безопасности, общественного порядка и безопасности, законных прав и интересов органоввласти, юридических и физических лиц; сбор электронных данных, относящихся к действиям по нарушению национальной безопасности, общественного порядка и безопасности, законных прав и интересов органов власти, юридических и физических лиц в киберпространстве; блокирование и ограничение работы информационных систем; приостановление ее работы; уголовное преследование в соответствии с Уголовно-процессуальным кодексом; другие меры в соответствии с положениями законов о национальной безопасности и законов об административных нарушениях.

Система обеспечения кибербезопасности Вьетнама активно обсуждается в мире и используется уже рядом государств для формирования национальной системы кибербезопаности. Представляется, что данная система может быть использована в Российской Федерации.

Литература

1. Заявление посольства США во Вьетнаме. [Электронный ресурс]. Режим доступа: https://vn.usembassy.gov/vi/pr08062018/. Дата обращения: 21.01.2019 г.

2. Luật An ninh mạng mới thông qua đưa VN trở về thời kỳ 'tăm tối'? (Новый закон о кибербезопасности возвращает Вьетнам к «темному»?). [Электронный ресурс]. Режим доступа: https://www.voatiengviet.com/a/luat-an-ninh-mang-moi-thong-qua-dua-vn-tro-ve-thoi-ky-tam-toi/4435296.html. Дата обращения: 21.01.2019 г.

3. Việt Nam nói luật an ninh mạng nhằm bảo vệ các quyền trên mạng (Вьетнам утверждает, что закон о кибербезопасности защищает права онлайн). [Электронный ресурс]. Режим доступа: https://www.voatiengviet.com/a/viet-nam-noi-luat-an-ninh-mang-bao-ve-cac-quyen-tren-mang/4489601.html. Дата обращения: 21.01.2019 г.

References

1. Zayavlenie posol'stva SShA vo V'etname. [Elektronnyj resurs]. Rezhim dostupa: https://vn.usembassy.gov/vi/pr08062018/. Data obrashcheniya: 21.01.2019 g.

2. Luật An ninh mạng mới thông qua đưa VN trở về thời kỳ 'tăm tối'? (Novyj zakon o kiberbezopasnosti vozvrashchaet V'etnam k «temnomu»?). [Elektronnyj resurs]. Rezhim dostupa: https://www.voatiengviet.com/a/luat-an-ninh-mang-moi-thong-qua-dua-vn-tro-ve-thoi-ky-tam-toi/4435296.html. Data obrashcheniya: 21.01.2019 g.

3. Việt Nam nói luật an ninh mạng nhằm bảo vệ các quyền trên mạng (V'etnam utverzhdaet, chto zakon o kiberbezopasnosti zashchishchaet prava onlajn). [Elektronnyj resurs]. Rezhim dostupa: https://www.voatiengviet.com/a/viet-nam-noi-luat-an-ninh-mang-bao-ve-cac-quyen-tren-mang/4489601.html. Data obrashcheniya: 21.01.2019 g.

МИНБАЛЕЕВ Алексей Владимирович, доктор юридических наук, главный научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права Российской академии наук. 119991, г. Москва, ул. Знаменка, д.10. E-mail: alexmin@bk.ru

MINBALEEV Aleksey, Doctor of Law, Chief Researcher of the Information Law and International information security Sector, Institute of State and Law of the Russian Academy of Sciences. 119991, Moscow, st. Znamenka, 10. E-mail: alexmin@bk.ru