КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ НАЦИОНАЛЬНОГО ИНТЕРНЕТА (ИРАНСКИЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ)

CYBERSECURITY IN THE CONTEXT OF THE NATIONAL INTERNET (THE IRANIAN EXPERIENCE OF COUNTERING CYBER THREATS)

УДК 343. 9

Ковалев Олег Геннадьевич, доктор юридических наук, кандидат психологических наук, профессор, профессор кафедры организации режима и оперативно-розыскной деятельности в уголовно-исполнительной системе, Псковский филиал Академии ФСИН России г. Псков.
Скипидаров Артем Алексеевич магистрант, ФГБОУ ВО Псковский государственный университет, г. Псков

Kovalev O. G., okovalev66@gmail.com
Skipidarov A. A. temapskov@yandex.ru

Аннотация

В статье рассматриваются особенности организации кибербезопасности в Исламской Республике Иран в условиях национального интернета. Проведенное исследование позволило выявить и описать создание национальной информационной сети, способной заменить в киберпространстве государства всемирную информационную, а также активное применение в этом контексте программ фильтрации и блокировки интернет- контентов и сайтов. В ходе исследования также было установлено, что иранская модель кибербезопасности как никакая другая базируется на идеологических принципах организации защиты от киберугроз и кибератак, функционировании исламского интернета, не допускающего распространение

враждебной для Республики политической, культурной или религиозной информации. Реализация проекта национального интернета состоит из трех основных этапов, реализованных и реализуемых в государстве, позволившими правительственным учреждениям на всей территории государства использовать в работе национальную сеть, а в исключительных случаях подключаться с помощью интернет-шлюза к всемирной сети Интернет. Другой особенностью защиты киберпространства Ирана от киберугроз и кибератак, влияющей на стратегию ее реализации, выявленной в ходе проведенного исследования, является высокая стоимость интернет услуг, по которой в соответствующем антирейтинге государств Исламская Республика занимает 8 позицию. Также заслуживает внимания и изучения иранский опыт применения специальной идентификационной системы функционирующей в режиме онлайн. Исследование организационных аспектов реализации кибербезопасности в Исламской Республике Иран показало, что система защиты киберпространства построена на сочетании использования возможностей и ресурсов государственных и негосударственных организаций и ведомств.мГлавным органом, координирующим сферу онлайн-коммуникаций, определяющим стратегию развития современных кибер и digital технологий является Верховный совет по киберпространству. Постоянно действующими рабочими органами совета являются национальный центр киберпространства, кибер-полиция, корпус стражей исламской революции, кибер-армия, комитет по определению случаев криминального контента и Министерство информационных и телекоммуникационных технологий.

Annotation

The article discusses the features of the organization of cybersecurity in the Islamic Republic of Iran in the context of the national Internet. The conducted research made it possible to identify and describe the creation of a national information network that can replace the global information network in the

cyberspace of the state, as well as the active use of programs for filtering and blocking Internet content and sites in this context. The study also found that the Iranian model of cybersecurity, like no other, is based on the ideological principles of organizing protection against cyber threats and cyber attacks, the functioning of the Islamic Internet, which does not allow the dissemination of political, cultural or religious information hostile to the Republic. The implementation of the national Internet project consists of three main stages, implemented and implemented in the state, which allowed government agencies throughout the state to use the national network in their work, and in exceptional cases to connect via an Internet gateway to the world Wide Web. Another feature of the protection of Iran's cyberspace from cyber threats and cyber attacks, which affects the strategy of its implementation, revealed in the course of the study, is the high cost of Internet services, for which the Islamic Republic occupies the 8th position in the corresponding anti-rating of states. The Iranian experience of using a special online identification system also deserves attention and study. A study of the organizational aspects of the implementation of cybersecurity in the Islamic Republic of Iran has shown that the cyberspace protection system is based on a combination of the use of the capabilities and resources of state and non-state organizations and departments.The Supreme Council for Cyberspace is the main body that coordinates the field of online communications and determines the strategy for the development of modern cyber and digital technologies. The permanent working bodies of the Council are the National Cyberspace Center, the Cyber Police, the Islamic Revolutionary Guard Corps, the Cyber Army, the Criminal Content Detection Committee, and the Ministry of Information and Telecommunications Technology.

Ключевые слова: кибербезопасность, Исламская Республика Иран, национальный интернет, национальная информационная сеть, киберпространство, фильтрация и блокировка, интернет- контенты, сайты, идеологические принципы, киберугрозы, кибератаки, исламский интернет, идентификационная система, Верховный совет по киберпространству,

национальный центр киберпространства, кибер-полиция, корпус стражей исламской революции, кибер-армия, комитет по определению случаев криминального контента, Министерство информационных и телекоммуникационных технологий.

Keywords: cybersecurity, Islamic Republic of Iran, national Internet, national information network, cyberspace, filtering and blocking, Internet content, sites, ideological principles, cyber threats, cyber attacks, Islamic Internet, identification system, Supreme Council for Cyberspace, National Cyberspace Center, Cyber police, Islamic Revolutionary Guard Corps, Cyber army, Committee for Determining Cases of Criminal content, Ministry of Information and Telecommunications Technologies.

Организация кибербезопасности в разных государствах сроится с учетом их экономического развития, наличия современных IT технологий, а также национальных традиций и идеологических особенностей. [1,2] В данном контексте особый исследовательский интерес представляет система защиты от киберугроз, внедряемая в последние годы в Исламской Республике Иран.

Проведенное теоретическое исследование методом сравнительного анализа литературных источников по теме позволило выявить и описать организационно-правовые особенности и направления реализации концепции кибербезопасности в названном государстве.

Основным отличием иранской модели кибербезопасности, выявленным в процессе исследования, является создание национальной информационной сети (так называемого «халяльного интернета»), которая по замыслу разработчиков должна заменить в киберпространстве государства всемирную информационную, а также активное применение в этом контексте программ фильтрации и блокировки интернет- контентов.

Иранская модель кибербезопасности как никакая другая базируется на идеологических принципах организации защиты от киберугроз и кибератак,

функционировании исламского интернета, не допускающего распространение враждебной для Республики политической, культурной или религиозной информации.

Работы по созданию национального интернета осуществляются на протяжении 16 лет и осложняются санкционной политикой США и других стран в отношении Ирана в сфере информационных технологий, приобретения хостинговых услуг.

Американские компании прекратили регистрацию национальных доменов «.ir» и «.com», одним из последствий которого стало приостановление обслуживания веб-сайта банка Bank Mellat Iran, поскольку работа онлайн-сервисов была приостановлена без предварительного резервного копирования данных. Данная ситуация оказала негативное влияние на имидж финансовой организации, вызвав панику клиентов и отток финансовых средств. После указанных событий правительство в целях безопасности перенесло все государственные веб-сайты на местный домен и услуги внутреннего хостинга.

Указанное событие и фиксируемые в последние десять лет многочисленные кибератаки на инфраструктуры Республики ускорили работы по созданию национального интернета, развитие технологий в сфере кибербезопасности (внутригосударственных межсетевых экранов для объектов критической инфраструктуры, ядерных, военных и экономических).

По замыслу разработчиков, реализация проекта национального интернета состоит из трех основных этапов. На первом, выполненном пять лет назад, была внедрена информационная инфраструктура, работающая самостоятельно, без взаимодействия с Интернетом. Проведенные технические мероприятия позволили открыть доступ к электронным государственным сервисам и внутреннему контенту.

На втором этапе были перенесены сервисы с внешних хостов на внутренние, которые затем были подключены к онлайн-системе новой информационной инфраструктуры. Тем самым было значительно увеличено

качество бизнес-серверов на основе современных IT технологий и digital ресурсов.

Третий этап предполагает апробацию и регулирование созданных информационных систем в национальной сети с использованием скоростного широкополосного доступа к домашнему контенту и сервисам.

Реализация указанных этапов позволила правительственным учреждениям на всей территории государства использовать в работе национальную сеть, а в исключительных случаях подключаться с помощью интернет-шлюза к всемирной сети Интернет.

Правительство Ирана обещает при запуске национального интернета в общегосударственном масштабе обеспечить права граждан, предоставив им право выбора способа выхода в Интернет.

Другой особенностью защиты киберпространства Ирана от киберугроз и кибератак, влияющей на стратегию ее реализации, выявленной в ходе проведенного исследования, является высокая стоимость интернет услуг, по которой в соответствующем антирейтинге государств Исламская Республика занимает 8 позицию. Стоимость интернет-трафика проводного интернета достигает 87 долларов США за 10 Мбит/сек. (в Российской Федерации в 16 раз меньше). При этом правительство страны планирует снизить стоимость интернет-трафика в программе национального интернета в два раза, а для интернет-провайдеров в десять раз, что, безусловно сделает его более привлекательным для различных категорий пользователей.

Также заслуживает внимания и изучения иранский опыт применения специальной идентификационной системы функционирующей в режиме онлайн и носящей название «шедевр». Названная система предназначена для обеспечения безопасности критической инфраструктуры государства и борьбы с киберпреступностью посредством идентификации отправляющих и получающих информацию пользователей по их IP адресу и национальным идентификационным номерам.

Исследование организационных аспектов реализации кибербезопасности в Исламской Республике Иран показало, что система защиты киберпространства построена на сочетании использования возможностей и ресурсов государственных и негосударственных организаций и ведомств.

Главным органом, координирующим сферу онлайн-коммуникаций, определяющим стратегию развития современных кибер и digital технологий является Верховный совет по киберпространству, успешно функционирующий более 9 лет. О статусе данной структуры говорит тот факт, что его работой руководит президент страны, а контролирует высшее духовное лицо государства – аятолла Хаменеи.

Членами совета являются руководители парламента (меджлиса), правительства, судебной власти, спецслужб и правоохранительных органов, армии, средств массовой информации (государственного радио и телевидения).

Постоянно действующими рабочими органами совета являются национальный центр киберпространства, кибер-полиция, комитет по определению случаев криминального контента и Министерство информационных и телекоммуникационных технологий.

Национальный центр киберпространства осуществляет мониторинг технологических, технических, методических, научных и политических событий происходящих во всемирном и национальном киберпространствах и контролирует исполнение решений Верховного совет по киберпространству.

Комитет по определению случаев криминального контента осуществляет цензуру в киберсети, блокирует выявленные криминальные и подозрительные интернет-контенты. Составляет списки сайтов, нарушающих общественную мораль, противоречащих устоям и принципам ислама, угрожающих национальной безопасности, критикующих государственных служащих либо организации, пропагандирующих преступную деятельность, осуществляющих контрмеры по разблокировке сайтов и интерент-контентов.

Кибер-полиция является элементом структуры полицейского управления и осуществляет противодействие таким распространенным киберпреступлениям как кража банковских данных, распространение фишинговых посланий и других.

Корпус стражей исламской революции, отвечающий за защиту исламских ценностей, существование и развитие политической системы государства также занимает важное место в защите киберпространства, выявлении, приостановке действия и ликвидации враждебных интернет-контентов. Данная структура также обеспечивает кибербезопасность интеренет-ресурсов от идеологического влияния, так называемого «культурного вторжения», оказываемого на иранское общество другими государствами.

В процессе проведенного исследования был определен такой важный элемент организационной структуры противодействия киберугрозам в иранской модели обеспечения кибербезопасности как кибер-армия, созданная 16 лет назад и представляющая собой кибер-сообщества законспирированных кибер-активистов, хакеров и блогеров, работающих в рассматриваемой сфере в интересах государственных структур. Они осуществляют мониторинг интернета, предупреждают, выявляют и купируют кибератаки на инфраструктурные объекты, атакуют оппозиционные и антиисламские интернет-контенты и сайты. Правительство отрицает свою причастность к деятельности указанных кибер-сообществ, одновременно констатируя что Исламская Республика Иран обладает развитой современной кибер-армией, занимающей четвертое место в рейтинге всех мировых держав.

Министерство информационных и телекоммуникационных технологий оценивает и анализирует информацию, поступающую из комитета по определению случаев криминального контента, регулирует процесс запуска Национальной информационной сети, управляет интернет сетью и коммуникационными инфраструктурами, поставляет интернет местным интернет-провайдерам.

Для реализации указанных функций в министерстве созданы такие структуры как:

- государственная компания телекоммуникационной инфраструктуры, обеспечивающая инфраструктуру для национальной сети и поставляющая интернет-услуги потребителям;
- агентство по регулированию коммуникаций, осуществляющее лицензирование телекоммуникационных технологий, предоставляющее лицензии интернет-провайдерам и отвечающее за контроль качества интернет-услуг, исполнение поручений правительства по фильтрации интернет-контента. [3]

Таким образом, проведенное изучение организационных аспектов защиты киберпространства по иранской модели, позволило выявит и описать основные преимущества и недостатки программы национального интернета, идеологическую основу, тактико-технологические приемы и методы противодействия вредоносным и враждебным интернет-контентам и сайтам, организационную структуру реагирования на киберугрозы и кибератаки, состоящую из государственных органов и киберсообществ, реализующих кибербезопасность в Исламской Республике Иран. Проанализированный опыт в данном направлении может быть полезен для совершенствования и развития отечественной стратегии кибербезопасности в современных условиях.

Литература

1. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты. Спб., изд-во Питер, 2017. – 254с.; Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности: международные и национальные стандарты / Учеб. пособие. Спб., изд-во Питер, 2019.-76с.

2. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы:

монография / В.М. Быков, В.Н. Черкасов. - Москва: Юрлитинформ, 2015.-325с.

3. Ссылка: www.pircenter.org [сайт]. – URL: https://www. pircenter.org/articles/2123-4833637 (дата обращения: 21.04.2021)

Literature

1. Rodichev Yu. A. Information security: regulatory and legal aspects. SPb., Pub. Pite, 2017. - 254p.; Rodichev Yu. A. Regulatory base and standards in the field of information security: international and national standards / Train. manual. SPb. Pub. Piter, 2019. - 76p.

2. Crimes in the field of computer information: criminological, criminal legal and criminalistic problems: monograph / V.M. Bykov, V.N. Cherkasov. - Moscow:Urlitinform, 2015.-325p.

3. Link: www.pircenter.org [site]. – URL: https://www. pircenter.org/articles/2123-4833637(accessed: 03.04.2021)