УДК 001.6

Кадыркулова Ж.Н.,
студент
2 курс, институт правоохранительной деятельности
Саратовская государственная юридическая академия
Россия, г. Саратов
Лескина Э.И.,
кандидат юридических наук, доцент
доцент кафедры «Информационного права и цифровых технологи»
Саратовская государственная юридическая академия
Россия, г. Саратов

ОСОБЕННОСТИ ИНФОРМАЦИОННО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В США.

Аннотация: *статья посвящена анализу развития национальной киберстратегии, а также действующих нормативно-правовых механизмов обеспечения кибербезопасности. Данная тема важна для понимания для понимания не только внутренней и внешнеполитической линии США, а также развития кибербезопасности в мире. Опыт США в обеспечении информационной безопасности является передовым, что обуславливает важность данного исследования.*

Ключевые слова: *информационная безопасность (кибербезопасность), информационно-правовое регулирование, информационная угроза, кибератаки, кибершпионаж.*

Annotation: *The article is devoted to the analysis of the development of the national cyber strategy, as well as the current regulatory and legal mechanisms for ensuring cyber security. This topic is important for understanding for understanding not only the domestic and foreign policy of the United States, but also the*

development of cybersecurity in the world. The US experience in providing information security is advanced, which determines the importance of this study.

Key words: *information security (cyber security), information and legal regulation, information threat, cyber attacks, cyber espionage*.

Политика США в области кибербезопасности формируется с начала 1990-х годов. Она включает в себя стратегии, процедуры и стандарты обеспечения безопасности киберпространства и проведения кибероперaций, охватывает полный комплекс мероприятий по минимизации угроз, снижению уровня уязвимости, реагированию на инциденты и восстановлению после них, а также действия на международном уровне, обеспечение доступности, целостности и безопасности информации, правоохранительную деятельность, дипломатические, военные и разведывательные миссии. Анализ развития национальной киберстратегии, а также действующих нормативно-правовых механизмов обеспечения кибербезопасности, представляется важным для понимания внешнеполитической линии США и развития кибербезопасности в мире.

Впервые еще в 1976 г. американский аналитик Томас Рона указал на то, что информационная инфраструктура становится ключевым компонентом экономики и одновременно одной из наиболее уязвимых целей как в военное, так и в мирное время[1].

На сегодняшний день от информационных технологий и информационной инфраструктуры зависит экономика и национальная безопасность США. Информационное пространство обеспечивает функционирование таких инфраструктур как транспорт, энергетика, финансы, здравоохранение, водоснабжение, сельское хозяйство, аварийные службы, военно-промышленная база. В этой связи основную озабоченность

[1] 8 Rona, Thomas P. Weapons Systems and Information War [Электронный ресурс] / Boeing Aerospace Company. Seattle, Washington. July 1976. – URL:

руководства США вызывают организованные кибератаки, в результате которых может быть нанесен урон национальной критической инфраструктуре, экономике или национальной безопасности[2].

Стоит отметить, что в 2013 году впервые в ежегодном докладе разведывательного сообщества США «Оценка глобальных угроз» киберугрозы заняли первое место в списке угроз национальной безопасности, опередив угрозу номер один – терроризм.[3]

Информационная угроза, связанная с деятельность человека бывает как умышленная, так и неумышленная.

Развитие, как следствие, роста числа угроз в киберпространстве потребовали от правительства страны разработки национальной стратегии по обеспечению безопасности киберпространства, которая включила бы в себя вопросы обеспечения безопасности критической инфраструктуры.

Представители разведслужбы США выделяют две группы киберугроз на основе деструктивных действий:

кибератаки – специальные наступательные операции, целью которых является достижение физического эффекта или воздействие на информацию, ее искажение и уничтожение, которые могут варьироваться от DDos атак («отказ доступа») на сайты до атак на объекты критической инфраструктуры, способных вывести их из строя на продолжительное время;

кибершпионаж – вмешательство в сети с целью получения доступа к чувствительной дипломатической, военной или экономической информации[4].

Федеральное бюро расследований (ФБР) в своей деятельности исходит из субъектного подхода и выделяет три основные группы акторов, представляющих угрозу в киберпространстве:

---

[2] The National Strategy to Secure Cyberspace. Washington D.C.: The White House. February 2003. – P. 6 [Электронный ресурс]. – URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (дата обращения: 10.02.14)

[3] Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence [Электронный ресурс] / Office of the Director of National Intelligence. Statement for the Record. March 12, 2013. – P. 1. – URL: http://www.intelligence.senate.gov/130312/clapper.pdf (дата обращения: 10.02.14)

[4] Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. March 12, 2013. – P. 1.

1. Организованные криминальные группы, которые в основном угрожают сектору финансовых услуг и постоянно повышают киберпотенциал.

2. Государства-спонсоры, которые заинтересованы в краже данных, включая интеллектуальную собственность и научно-исследовательские разработки предприятий, государственных институтов и подрядчиков.

3. Террористические группы, использующие сетевые технологии в целях проведения деструктивных действий в отношении критической инфраструктуры страны, и тем самым представляющие угрозу национальной безопасности США[5].

Министерство обороны США (МО) в своей деятельности исходит из четырех категорий угроз кибербезопасности, которые включают в себя как акторов, так и отдельные действия:

- угрозы, исходящие от внешних акторов (иностранных государств, криминальных групп)

- угрозы, исходящие от внутренних акторов (инсайдеров);

- угрозы, связанные с уязвимостью сети поставщиков оборудования и программного обеспечения;

- угрозы функциональной деятельности Министерства166. Ведомственный подход демонстрирует, что на практике видение угроз информационной безопасности во многом определяется задачами, входящими в компетенцию той или иной федеральной структуры. При этом угрозы, исходящие от действий государств, преступников и террористов, относятся к зоне ответственности сразу нескольких министерств и ведомств, что определяет необходимость обеспечения межведомственного взаимодействия по вопросам обеспечения информационной безопасности.

[5] The Cyber Threat: Part 1. On the Front Lines with Shawn Henry [Электронный ресурс] / Federal Bureau of Investigation. March 27, 2012. – URL: http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712 (дата обращения: 12.03.2014).

Выявление групп угроз информационной безопасности позволит получить целостное виденье политики США в сфере обеспечения безопасности информационного пространства.

Первые шаги в разработке комплексной стратегии были предприняты администацией Дж. Буша-мл. В «Национальной стратегии по обеспечению безопасности киберпространства»[6] В качестве стратегических целей были определены:

- предупреждение кибератак на критическую инфраструктуру США;
- снижение уровня уязвимости к кибератакам;
- минимизация ущерба и времени восстановления после кибератак

Для достижения данных целей были выделены программы и направления обеспечения безопасности киберпространства:

1. Национальная система реагирования на инциденты безопасности киберпространства.

2. Национальная программа снижения уязвимости и угроз безопасности киберпространства.

3. Национальная программа обучения и повышения осведомленности о безопасности киберпространства.

4. Обеспечение безопасности правительственных информационных систем.

Таким образом, в данной Стратегии был сформулирован важный принцип обеспечения кибербезопасности – снижение риска проведения кибератак против США посредством упреждающих действий, которые, в свою очередь, могут предусматривать проведение широкого спектра информационных операций.

« В дальнейшем положения «Комплексной инициативы» легли в основу киберполитики Б. Обамы. опытом. Администрация Обамы сделала

[6] The National Strategy to Secure Cyberspace (PDF). U.S. government via Department of Homeland Security (February 2003). Дата обращения 18 мая 2008. Архивировано 12 февраля 2008 года.

международное взаимодействие центральным элементом своей программы по кибербезопасности. В 2010 г. в стенах ООН США приняли участие в создании первоначального формата международного сотрудничества.

В США была разработана и опубликована Международная стратегия по киберпространству, призванная обеспечить единую основу для международного взаимодействия по вопросам киберпространства и использовать для этого все доступные инструменты влияния, в том числе дипломатические, военные и экономические[7]. В том числе и для реализации этой стратегии Государственный департамент США объявил о создании должности старшего координатора по вопросам киберпространства. С первых дней президенства Б.Обама, определил сферу кибербезопасности, как один из главных приоритетов, взяв курс на пересмотр политики США в области обеспечения кибербезопасности ,

В мае 2009 года группа экспертов представила президенту «Обзор киберполитики» (Cyberspace Policy Review), в котором предлагались дальнейшие шаги, направленные на внутренние преобразования системы кибербезопасности.

По итогам Обзора можно выделить основные направления в области обеспечения кибербезопасности

- создание механизмов совместных действий между федеральными и местными органами власти, а также частным сектором, в целях обеспечения единого и организованного подхода к ответным мерам на кибератаки;

- укрепление сотрудничества государственного и частного секторов для обеспечения технических решений в области безопасности;

- проведение передовых исследований и разработок в области ИКТ;

[7] International Strategy for Cyberspace // White House. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения: 15.10.2011

- повышение информированности и грамотности населения, инвестиции в НИОКР, образовательные программы в школах и университетах[8]».

Угрозы кибербезопасности могут нести угрозу международному миру, по мере того, как традиционные формы конфликтов переносятся в киберпространство. Соединенные Штаты готовы противодействовать им, придерживаясь при этом основных принципов, на которых остановимся подробнее.

Основные свободы. В киберпространстве наибольшую релевантность получает возможность искать, получать и передавать информацию и идеи посредством любой доступной среды, невзирая на существующие границы. В то же время США не закрывают глаза на тех пользователей Интернета, которые имеют недоброжелательные намерения, однако уточняют, что исключения для принципов свободы слова в киберпространстве должны подбираться самым тщательным образом. «Например, детской порнографии, актам неопровержимой жестокости или организациям, пропагандирующим терроризм, не место в любом обществе, соответственно нет места им и в Интернете».

Личная тайна. По мере того, как граждане все активнее вносят Интернет в свою общественную и частную жизнь, они должны иметь представление о том, каким образом могут быть использованы их личные данные. В равной степени они имеют право на защиту от мошенничества, хищений и угроз личной безопасности, и ожидают отслеживания и пресечения деятельности тех пользователей, которые с помощью Интернета обманывают остальных граждан. Соединенные Штаты уверены, что между двумя противоположностями — защитой конфиденциальной информации одних и необходимостью слежения за такой же информацией других граждан можно найти определенный баланс.

[8] https://mgimo.ru/files2/y01_2015/261815/diss-batueva-final-corr.pdf

Свободные потоки информации. США убеждены, что государства не должны выбирать между свободным потоком информации и безопасностью своих сетей. Утверждается, что «лучшие решения в области кибербезопасности отличаются динамичностью и высокой приспосабливаемостью при минимальных последствиях для рабочих параметров сети», а применение устанавливаемых на национальном уровне фильтров и защитных экранов является лишь иллюзией безопасности. При этом очевидно, что на данный момент указанные «передовые решения» в массовом порядке не применяются. Принцип беспрепятственного потока информации, как и принцип полной анонимности, несовместим с эффективным обеспечением правопорядка, защитой детей и безопасностью инфраструктур. США сталкиваются с задачей, поддержания открытой и либеральной среды, которая способствует, с одной стороны, росту эффективности, экономическому процветанию и свободной торговли, а с другой — обеспечивает безопасность и защищенность.

В связи с обострившимся конфликтом между Китаем и США по поводу выявленного инцидента с кибершпионажом, в марте Обамой был одобрен закон «О консолидированных и дальнейших ассигнованиях». Закон содержал положение о кибербезопасности, согласно которому национальное космическое агентство НАСА, министерство юстиции и торговли США, а также Национальный научный фонд могут приобретать технологические системы, произведенный или собранные организациями, принадлежащими, управляющимися или получающими субсидии со стороны Китайской народной республики, только после того, как будет принято решение оценочным органом (главой агентств закупок), что данная закупка соответствует национальным интересам США. Из этогоследует, что в целях кибербезопасности США готовы использовать меры экономического характера, направленные против конкретной страны.

На данный момент США активизирует работу в области законотворчества, уделяя существенное внимание созданию необходимых механизмов взаимодействия внутри федеральных ведомств, так и между частными и государственными секторами, в целях повышения уровня кибербезопасности.

Анализ нормативно-правовой базы позволяет выявить основные тенденции усовершенствования национальной системы обеспечения информационной безопасности:

1. Совершенствования государственных механизмов обеспечения информационной безопасности, направленное на исключение дублирования функций федеральных министерств и ведомств.

2. Усиление контроля над киберпространством со стороны государственных органов и повышение роли силовых ведомств. Законодательство США обеспечивает достаточную свободу действий спецслужб и правоохранительным органам для обеспечения мониторинга и слежения в информационном пространстве.

3. Совершенствование правовых механизмов обеспечения информационной безопасности, направленное на противодействие основным видам злоупотребления ИКТ, как на национальном, так и на международном уровне. США ведут работу за повышением уровня ответственности федеральных органов, компаний и отдельных пользователей, а обеспечение кибербезопасности.

4. Наращивание киберпотенциала. Согласно президентским директивам и документам Министерства обороны, основной целью США является обеспечение информационного превосходства над противником.

Итак, США одними из первых начали относиться к кибербезопасности как к задаче стратегической важности, что повлияло на информационно правовое регулирование во всех странах. Экономически и информационно-развитые страны, такие как США, задают тон информационно-правового

регулирования стран на международной арене. Информационно-правовое регулирование необходимая, несомненно, важная вещь в современном мире, т.к. общество, на рубеже веков, входит в новое информационное пространство, которое необходимо регулировать, как на уровне страны, так и на международном уровне.

В заключении отметим, что развитие информационно-коммуникационных технологий предопределяет конкурентоспособность любого государства на мировой арене, способствует экономическому развитию, а также эффективную деятельность в разнообразных областях[9]. В любой стране мы можем наблюдать пробелы решения проблем в информационно-правовых отношениях. Мы считаем, что в недалеком будущем страны смогут сделать общую стандартную сферу и правила поведения регулирования информационно-правовых отношений.

Список литературных и нормативных источников:

1. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // Рос. газета. – № 4131. – 2006. – 29 июля.

2. Computer Fraud and Abuse Act of 1984. Public Law 98-473, 98 Stat. 2190. 18 U.S.C. 1030 [Электронный ресурс]. – URL: http://www.gpo.gov/fdsys/granule/USCODE-2010-title18/USCODE-2010-title18-partI-chap47- sec1030/content-detail.html

3. The Cyber Threat: Part 1. On the Front Lines with Shawn Henry [Электронный ресурс] / Federal Bureau of Investigation. March 27, 2012. – URL: http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712 (дата обращения: 12.03.2014).

[9] Лескина Э.И. Применение блокчейн-технологий в сфере труда // Юрист. 2018. № 11. С. 25-30.

4. The National Strategy to Secure Cyberspace (PDF). U.S. government via Department of Homeland Security (February 2003). Дата обращения 18 мая 2008. Архивировано 12 февраля 2008 года.

5. The National Strategy to Secure Cyberspace (PDF). U.S. government via Department of Homeland Security (February 2003). Дата обращения 18 мая 2008. Архивировано 12 февраля 2008 года.

6. Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. March 12, 2013. – P. 1.

7. Лескина Э.И. Влияние развития нейронных сетей на трудовые отношения // Российская юстиция, 2020, № 8, С. 9-12.

8. Лескина Э.И. Применение блокчейн-технологий в сфере труда // Юрист. 2018. № 11. С. 25-30.