



УДК 34.03:004.056.5

ББК Х401.114 + Х401.011.1:Х401.114

Дубровин О. В.

К ВОПРОСУ ГОСУДАРСТВЕННОЙ КИБЕРБЕЗОПАСНОСТИ

В статье рассмотрены некоторые элементы кибербезопасности Соединенных Штатов Америки, организаций Североатлантического договора, основы стратегии кибербезопасности России, а так же предложения по защите информационного пространства Российской Федерации. Автор приходит к выводу о необходимости принятия и реализации стратегии кибербезопасности России в ряду первоочередных и стратегических вопросов Правительства Российской Федерации, а также необходимости объединения усилий государств в разработке и принятии международных конвенций по вопросам кибербезопасности.

Ключевые слова: кибербезопасность, государственная кибербезопасность, стратегия кибербезопасности России.

Dubrovin O. V.

TO THE QUESTION OF THE STATE CYBER SECURITY

The article considers certain aspects of cyber security of the United States of America, organizations of the North American Treaty, fundamental strategies of cyber security in Russia, as well as the proposals on the information security in the Russian Federation. The author concludes the necessity of the realization of the strategy of cyber security in Russia as a top priority issue for the Government of the Russian Federation, as well as the necessity of the integrating efforts in the development of international conventions on the questions of cyber security.

Keywords: cyber security, state cyber security, strategy of cyber security in Russia.

Развитие информационных и телекоммуникационных технологий, расширение и доступность интернет-пространства, его использование гражданами, бизнесом, органами государственной и муниципальной власти – эти и многие другие факторы заставляют задуматься о кибербезопасности как об одной из ключевых составляющих национального суверенитета Российской Федерации.

Частные компании и государственные учреждения, некоммерческие организации и политические партии, города-государства и ведущие страны мира, все сталкиваются с

реальными проявлениями угроз кибербезопасности, беспрецедентными по своему масштабу, разнообразию и сложности.

В Интернете не проведены границы государств, куда можно было бы выставить в охранение караулы, в связи с этим остается открытым вопрос поиска и привлечения к ответственности лиц, нарушающих законы с применением интернет-пространства, информационных и телекоммуникационных технологий.

Следует согласиться с мнением Бирюковой Т. А., Беляковой Е. Г., Копьева А. В., Морозова С. Ю., Хлистун Ю. В., Юдиной А. Б., которые считают,

что при создании и использовании российских сегментов систем глобальной подвижной персональной спутниковой связи должны приниматься исчерпывающие меры по обеспечению информационной безопасности, исключающие ухудшение качественных характеристик функционирования российского сегмента, неконтролируемое его использование и блокирование его работы по конъюнктурным или политическим мотивам, что может приводить к нанесению ущерба пользователям и владельцу российского сегмента и интересам национальной безопасности и суверенитету РФ¹.

При этом требования по обеспечению одного из важнейших элементов информационной безопасности – российских сегментов указанных систем – установлены в 1999г.²

Представляется необходимым рассмотреть мировой опыт решения данной проблемы.

Одним из лидеров в области обеспечения информационной безопасности и контроля над глобальной сетью Интернет 26 мая 2010 года была опубликована «Стратегия национальной безопасности Соединенных Штатов»³.

Согласно указанному документу спектр военных угроз остается широким, включая угрозы в космосе и в киберпространстве, таким же широким является спектр потенциальных противников, от целых государств до негосударственных организаций.

Угрозами для внутренней безопасности названы широкомасштабные кибератаки. При этом в Стратегии национальной безопасности Соединенных Штатов отмечено, что особую важность имеет защищенность киберпространства, поскольку от этого зависит и гражданский (личностная безопасность, экономика, торговля, инфраструктура жизнеобеспечения), и военный сектор⁴.

Следует отметить, что Соединенные Штаты Америки стремятся завоевать главенствующее положение в мире, особое внимание уделяют глобальному информационному пространству, создавая военное киберкомандование.

В американской трактовке контроль над киберпространством означает защиту собственных информационных систем и хранящейся в них информации, а также способность вести наступательные кибернетические операции. При этом, согласно официально принятому в США определению, под кибернетическим пространством понимается некое условное (виртуальное) пространство, возникающее в процессе использования электронных и электромагнитных средств хранения, обработки и обмена дан-

ными в компьютерных сетях и связанных с ними физических инфраструктурах⁵.

Согласно отчету, подготовленному по результатам ежегодного саммита по угрозам в киберпространстве, прошедшего 15 октября 2008 года, определен перечень наиболее серьезных киберугроз. К их числу было отнесено:

- распространение вирусных программ, способных наносить ущерб программному и аппаратному обеспечению;
- скрытое дистанционное управление информационными системами (перегрузка каналов, рассылка спама, хищение информационных ресурсов);
- активизация боевых действий в киберпространстве;
- перехват IP-адресов и мобильного телефонного трафика;
- экономическая и финансовая преступность в кибернетическом пространстве⁶.

В 2011 году организацией Североатлантического договора (НАТО) была принята Доктрина кибербезопасности, текст которой на сегодняшний день не представлен широкому кругу лиц. При этом организацией Североатлантического договора создаются органы коллективной кибербезопасности:

- Совет по киберобороне (NATO Cyber Defence Management Board – CDMB) для координации вопросов обороны в киберпространстве в штаб-квартире НАТО основных командных центров Организации;
- Совет по консультациям, контролю и командованию (The NATO Consultation, Control and Command – NC3) как основной орган, отвечающий за технические и прикладные аспекты киберобороны;
- Военное руководство НАТО (NATO Military Authorities – NMA) и Агентство по консультациям, контролю и командованию (Consultation, Control and Command Agency – NC3A) имеют определенные полномочия по определению стандартов оборонного потенциала в области кибербезопасности, а также закупок для его развития;
- Агентство по связи и информационным услугам НАТО (NATO Communication and Information Services Agency – NCSA) отвечает за предоставление технических и оперативных услуг в области кибербезопасности по всей организации Североатлантического договора. Агентство отвечает за противодействие любой киберагрессии против членов НАТО⁷.

Специализированный центр по обороне в сфере кибербезопасности НАТО (CCDCOE) в Таллине при участии 20 экспертов и консультантов

– сотрудников Международного комитета Красного Креста и Киберкомандования США разработал пособие о ведении санкционированных онлайн-атак.

Согласно принципам спланированной хакерской атаки, указанным в пособии, нападениям не должны подвергаться такие важные гражданские объекты, как больницы, дамбы и атомные электростанции, при этом атаки на ключевые гражданские объекты могут рассматриваться как нарушения Женевской конвенции⁸.

Руководитель экспертной группы по созданию пособия Майкл Шмитт заявил, что применение силы возможно только в том случае, если разразился вооруженный конфликт⁹. В документе также рассмотрены и вопросы поиска инициаторов атаки.

Представляется необходимым отметить интерес Соединенных Штатов Америки в заключении соглашений по вопросам кибербезопасности со странами, не являющимися участниками Североатлантического договора.

В апреле 2013 г. приняли решение начать диалог по вопросу кибербезопасности Соединенные Штаты Америки и Китай, которые на протяжении последних лет обвиняли друг друга в хакерских атаках.

Исключением не является и Российская Федерация. В июне 2013 г. между Правительством Соединенных Штатов Америки и Правительством Российской Федерации было заключено соглашение об организации линии прямой шифрованной связи между уполномоченными представителями Соединенных Штатов Америки и Российской Федерации по вопросам угроз в сфере использования информационно-коммуникационных технологий и самим информационно-коммуникационным технологиям¹⁰.

Главная опасность виртуальных кибератак есть возможность наносить дистанционный реальный урон экономической и политической независимости государства средствами информационных и телекоммуникационных технологий.

Все большее количество жизнеобеспечивающей инфраструктуры государства – электронное правительство, платежные системы, он-лайн-банкинг, интернет-трейдинг и т.д. – становится потенциальными объектами для кибератак. Например, программные закладки в программном обеспечении компьютеров в посольстве станут отправлять секретные данные злоумышленникам, которые смогут выставить их на продажу. Кража баз данных банка может привести к массовому выводу денег со счетов населения. Киберугрозам может подвергаться кто угодно – госу-

дарство в целом, предприятия и организации, личность, все это может оказать влияние на независимость государства.

При рассмотрении данного вопроса следует обратить внимание на деятельность Временной комиссии Совета Федерации по развитию информационного общества, председателем которой является член Совета Федерации Федерального Собрания Российской Федерации Р. У. Гаттаров.

В марте 2013 г. при инициативе членов Временной комиссии Совета Федерации по развитию информационного общества был разработан проект национальной Стратегии кибербезопасности России¹¹, в котором были определены основные угрозы в области кибербезопасности:

- 1) разработка и применение информационного оружия, подготовка и ведение информационной войны;
- 2) информационный терроризм;
- 3) информационная преступность;
- 4) кибершпионаж (таргетированные атаки на информационные массивы государственных структур, бизнеса и граждан)
- 5) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности государства, бизнеса, гражданина;
- 6) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде;
- 7) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

К основным направлениям Стратегии кибербезопасности России были отнесены:

- 1) безопасность онлайн-бизнеса. Исследование «Экономика Рунета» показало, что объем российского сегмента интернет-рынка достигает 1% ВВП с прогнозом роста в 30% в год. Со стороны государства необходимо оказывать определенную поддержку этому рынку, как, например, делают в США. Прежде всего речь идет о защите финансовых онлайн-операций, противостоянии и расследовании киберпреступлений;
- 2) обеспечение гарантий прав граждан. Каждый все больше доступен по каналам цифровой коммуникации, и потому более уязвим. Растет количество случаев онлайн-мошенничества, краж персональных данных, преследования. Гражданин должен иметь право на защиту его личной жизни и данных;

3) защита национальной информационно-коммуникационной инфраструктуры. Речь идет как об органах государственного управления, так и крупных объектах, таких, как атомные станции и трубопроводы;

4) реализация современных систем управления с использованием информационно-коммуникационных технологий. Электронное правительство, электронный парламент, электронные выборы – все эти инновационные системы могут быть очень уязвимы для манипуляций по каналам цифровой коммуникации. Это очень опасно, т. к. нарушается функционирование ключевых государственных механизмов и теряется управляемость, поэтому нужно обеспечить их защищенность;

5) построение эффективных механизмов борьбы с киберпреступлениями. Сегодня расследуется малая доля киберпреступлений, и практически все они – на нашей территории. Наиболее опасные операции проводятся с территорий других государств, поэтому расследование и привлечение ответственности сильно усложняется, поскольку дело выходит на международный уровень. Для решения проблемы нужно ратифицировать Конвенцию по борьбе с киберпреступностью;

6) противодействие массированным кибератакам. США, страны Западной Европы, Китай, Южная Корея и другие страны активно развивают свои службы по ведению киберопераций. Они включают как оборону, так и нападение. России необходимо быть готовой защищать свои цифровые границы от краж секретных данных, которые налажены в фоновом режиме, и нанесения ущерба в случае обострения отношений.

Следует отметить, что в целях защиты информационного пространства Российской Федерации стратегией кибербезопасности России предложено:

1) создание государственного ситуационного центра, функционирующего в режиме 24/7, с целью изучения киберугроз и реагирования на них;

2) создание портала, содержащего статистическую информацию об инцидентах в сфере кибербезопасности, потенциальных уязвимостях информационных систем и способах их компенсации, а также предоставляющего гражд-

дам РФ возможность публиковать сообщения о проблемах в области кибербезопасности, обсуждать их и предлагать конструктивные решения, получать обратную связь от уполномоченных государственных органов;

3) организация национальных учений в области кибербезопасности с участием военных подразделений, правоохранительных органов, государственных органов, а также руководства критически важных объектов;

4) полноценный запуск и переход на широкое использование инфраструктуры электронной цифровой подписи;

5) разработка и принятие государственных стандартов кибербезопасности Российской Федерации, а также реализация механизмов их регулярного пересмотра в соответствии с лучшими мировыми практиками и новейшими технологиями;

6) предоставление правоохранительным органам полномочий, расширяющих их оперативные возможности по борьбе с киберугрозами;

7) принятие программы развития отечественных программных средств обеспечения кибербезопасности;

8) обязательная публикация под свободной лицензией ПО, разработанного по госзаказу (кроме особых случаев);

9) пересмотр квалификационных требований к государственным служащим в области информационных технологий с учётом современных тенденций отрасли.

Представляется необходимым высоко оценить профессионализм и актуальность разработки стратегии кибербезопасности России, при этом считаем, вопрос ее принятия и реализации должен входить в перечень первоочередных и стратегических вопросов Правительства Российской Федерации.

Также следует отметить необходимость объединения усилий государств в разработке и принятии международных Конвенций по вопросам кибербезопасности в целях совершенствования законодательной базы и снижения барьеров при поиске и поимке киберпреступников, обеспечения национальной безопасности стран.

Литература

¹ Бирюкова Т. А., Белякова Е. Г., Копьев А. В., Морозов С. Ю., Хлистун Ю. В., Юдина А. Б. Комментарий к Федеральному закону от 7 июля 2003 г. № 126-ФЗ «О связи» // СПС «ГАРАНТ». 2012.

² Об утверждении Положения о порядке, общих условиях и принципах использования на территории Российской Федерации систем глобальной подвижной персональной спутниковой связи (ГППСС) и требованиях по обеспечению информационной безопасности для российских сегментов указанных систем»: Приказ Гостелекома РФ от 21 июля 1999 г. № 22 // Российская газета. 1999. № 247.

³ U.S. National Security Strategy 2010 // National Strategy Forum URL: <http://www.nationalstrategy.com/NSFReview/Winter2009Vol19No1USNSS2010.aspx> (дата обращения: 15.09.2013 г.).

⁴ Конышев В. Н., Сергунин А. А. Стратегия национальной безопасности Б. Обамы: старое вино в новых мехах? // *Обозреватель – Observer*. 2010. № 12 (251).

⁵ Бедрицкий А. В. Американская политика контроля над кибернетическим пространством // Москва. 2012. № 6.

⁶ Там же.

⁷ КИБЕРКОМ займется конфликтом Google и Китая // Интернет-портал. Независимая газета. URL: http://nvo.ng.ru/forces/2011-10-07/11_cybercom.html (дата обращения: 15.09.2013 г.).

⁸ Женевская Конвенция о защите гражданского населения во время войны // Действующее международное право. 2007. т. 2.

⁹ Искусство кибервойны: НАТО выпустила руководство для хакеров. // Интернет-портал ТВ-новости. URL: <http://russian.rt.com/article/5929> (дата обращения: 15.09.2013 г.).

¹⁰ О заключении Соглашения между Правительством Российской Федерации и Правительством Соединенных Штатов Америки об организации линии прямой шифрованной связи между уполномоченными представителями Российской Федерации и Соединенных Штатов Америки по вопросам угроз в сфере использования информационно-коммуникационных технологий и самим информационно-коммуникационным технологиям: Распоряжение Правительства РФ от 15 июня 2013 г. № 983-р. // СЗ РФ. 2013. № 25. ст. 3196.

¹¹ Проект Стратегии национальной кибербезопасности РФ. Интернет-портал. URL: <http://gattarovruslan.ru/?dir=initiative&index=4> (дата обращения: 15.09.2013 г.).

References

¹ Biryukova T.A., Belyakova E.G., Kop'ev A.V., Morozov S.Yu., Khlistun Yu.V., Yudina A.B. Kommentarii k Federal'nomu zakonu ot 7 iyulya 2003 g. № 126-FZ «O svyazi» [Commentaries to the Federal Law as of July 7, 2003 No. 126-Fz 'On communications'] // *Sistema GARANT*. - 2012.

² Ob utverzhenii Polozheniya o poryadke, obshchikh usloviyakh i printsipakh ispol'zovaniya na territorii Rossiiskoi Federatsii sistem global'noi podvizhnoi personal'noi sputnikovoi svyazi (GPPSS) i trebovaniyakh po obespecheniyu informatsionnoi bezopasnosti dlya rossiiskikh segmentov ukazannykh sistem»: Prikaz Gostelekoma RF ot 21 iyulya 1999 g. № 22 [On the affirmation of the provision on procedures, general interpretation and principles of the use of the systems of global portable personal satellite communications and security requirements for the Russian segments of the abovementioned systems: Order of the State Telecommunication Agency of the Russian Federation as of July 21, 1999 No.22] // *Rossiiskaya gazeta* [Russian post]. 1999. No. 247.

³ U.S. National Security Strategy 2010 // National Strategy Forum URL: <http://www.nationalstrategy.com/NSFReview/Winter2009Vol19No1USNSS2010.aspx> (data obrashcheniya: 15.09.2013g.).

⁴ Konyshev V.N., Sergunin A.A. Strategiya natsional'noi bezopasnosti B. Obamy: staroe vino v novykh mekhakh? [Strategy of national security of Barak Obama: Old wine in new bottles?] // *Obozrevatel'–Observer*. 2010. No. 12 (251).

⁵ Bedritskii A.V. Amerikanskaya politika kontrolya nad kiberneticheskim prostranstvom [American policy of control over cyber space] // *Moscow*. 2012. No. 6.

⁶ Bedritskii A.V. Amerikanskaya politika kontrolya nad kiberneticheskim prostranstvom [American policy of control over cyber space] // *Moskva*. 2012. No. 6.

⁷ КИБЕРКОМ займется конфликтом Google и Китая [CYBERCOM will manage the conflict of Google and China] // Интернет-портал. Независимая газета. URL: http://nvo.ng.ru/forces/2011-10-07/11_cybercom.html (date of compellation: 15.09.2013g.).

⁸ Zhenevskaya Konventsiya o zashchite grazhdanskogo naseleniya vo vremya voiny [Geneva Convention Relative to the Protection of Civilian Persons in Time of War] // *Deistvuyushchee mezhdunarodnoe pravo* [Present international law]. 2007. V. 2.

⁹ Iskusstvo kibervoiny: NATO vypustila rukovodstvo dlya khakerov [The art of cyber war: NATO has issued the guidance for hackers] // Интернет – портал ТВ-новости. URL: <http://russian.rt.com/article/5929> (date of compellation: 15.09.2013).

¹⁰ O zaklyuchenii Soglasheniya mezhdu Pravitel'stvom Rossiiskoi Federatsii i Pravitel'stvom Soedinennykh Shtatov Ameriki ob organizatsii linii pryamoi shifrovannoi svyazi mezhdu upolnomochennymi predstavitel'yami Rossiiskoi Federatsii i Soedinennykh Shtatov Ameriki po voprosam ugroz v sfere ispol'zovaniya informatsionno-kommunikatsionnykh tekhnologii i samim informatsionno-kommunikatsionnykh tekhnologiyam: Rasporyazhenie Pravitel'stva RF ot 15 iyunya 2013 g. № 983-r. [On conclusion of the agreement between the Government of the Russian Federation and the Government of the United States of America on the establishment of the line of direct cypher communication between the authorized representatives of the Russian Federation and the United States of America on the issues of threats in the sphere of the use of information and communication technologies: Decree of the Government of the Russian Federation as of June 15, 2013 No. 983-r] // *SZ RF* [Official Gazette of the Russian Federation]. 2013. No. 25. Art. 3196.

¹¹ Proekt Strategii natsional'noi kiberbezopasnosti RF [Project of the strategy of national cyber security of the Russian Federation]. Internet portal. URL: <http://gattarovruslan.ru/?dir=initiative&index=4> (date of compellation: 15.09.2013).

Дубровин Олег Владимирович, кандидат юридических наук, доцент кафедры конституционного и административного права Южно-Уральского государственного университета, 454136, г. Челябинск, пр. Победы, д. 293, кв. 339, т. м.+79128082228. E-mail: dov1974@mail.ru.

Dubrovин Oleg Vladimirovich, Candidate of Juridical Sciences, The Associate Professor of Constitutional and Administrative Law, South Ural State University, 454136, Chelyabinsk, Pobedy Prospect, B.293, Apt. 339, bw: +79128082228. E-mail: dov1974@mail.ru.