

11. Долгова Д. А. Иран между Россией и США // Актуал. проблемы совр. международ. отношений. 2015. № 6. С. 75–81.

12. Рыжов И. В., Бородин М. Ю. «Арабская весна» как квинтэссенция межарабских противоречий // Вестн. Нижегород. ун-та им. Н. И. Лобачевского. 2012. № 6. С. 252–256.

13. Шаклеина Т. А., Панов А. Н., Булатов А. С. Внешняя политика России. 1991–2016 : кол. монография / под общ. ред. и с предисл. акад. А. В. Торкунова. М. : МГИМО-Университет, 2017. 538 с.

УДК 323.22/.28

Владимир Андреевич Михеев,
студент 4-го курса бакалавриата
Уральского гуманитарного института
Уральский федеральный университет

КИБЕРПРЕСТУПНОСТЬ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ РЕСПУБЛИКИ КОРЕЯ И МЕРЫ ПРОТИВОДЕЙСТВИЯ ЕЙ СО СТОРОНЫ ГОСУДАРСТВА

Статья посвящена анализу такого социального явления, как киберпреступность в Республике Корея, а также мер противодействия ему со стороны государства: органов военного управления, законодательного аппарата. Проблема преступлений в сфере компьютерной информации на данный момент является крайне актуальной для всего мирового сообщества, в том числе и для Южной Кореи, страны с одним из наиболее развитых сегментов Интернета в мире.

Ключевые слова: киберпреступность, Республика Корея, кибервойны, КНДР, Интернет, компьютерные технологии.

CYBERCRIME IN THE INTERNET OF THE REPUBLIC OF KOREA AND STATE COUNTER-MEASURES

The article is devoted to the analysis of the phenomenon of cybercrime in the Republic of Korea, as well as measures to counter it by the state, both from the military and from the legislative apparatus. The problem of computer crime at the moment is extremely important for the entire world community, including South Korea — country with one of the most developed segments of the Internet in the world.

Keywords: cybercrime, Republic of Korea, cyberwar, DPRK, Internet, computer technology.

«Киберпреступность» — преступления в отношении отдельного лица или группы лиц, с целью умышленно нанести физический, моральный вред, используя компьютерные технологии [1, р. 32]. Это — проблема мирового масштаба, и ее решение возможно только при объединении усилий государств [2, с. 43]. Исследования о киберпреступности актуальны — в начале XXI в. в России, за рубежом имелись исследования по этой теме [3, с. 2]. Данную проблему стоит рассмотреть на примере страны с развитыми интернет-технологиями.

Республика Корея (далее РК) — одна из таких. Это страна с развитыми интернет-технологиями. Их использует более 90 % граждан, а скорость соединения — одна из самых высоких в мире [4]. Развитие активно идет еще с 1997 г. [5, с. 12]. Интернет внедрен и в государственный аппарат РК [6]. Но, по данным международного рейтинга Cyber Risk Score 2014, РК в Азиатско-Тихоокеанском регионе — самая слабо защищенная от «кибератак» страна [7]. Поэтому проблема кибербезопасности для нее крайне актуальна. В данной статье будет рассмотрено явление киберпреступности в период, начиная с 2010 г. — переломного для страны в этом плане.

Начать следует с законодательной активности РК. В стране существуют специальные законы для регулирования киберсферы. Конвенция Совета Европы по киберпреступлениям подписана в 2001 г., но единого мнения у мирового сообщества по этой проблеме нет [8, с. 54]. Основным законом РК для регулирования сети Интернет является «Закон о содействии использованию информационно-коммуникационных сетей и защите информации», используемый наряду с основным Уголовным кодексом РК [9].

Количество киберпреступлений в стране уже в 2012 г. превысило отметку в 80 тыс.: распространение «контента для взрослых», «агитация в пользу КНДР» или нарушения авторских прав. «Более опасный» криминал в Сети не присутствует [10, с. 57]. Приоритетов в «защите Интернета» у Южной Кореи два.

Первый — «оборона» от воздействия КНДР. Материалы о Северной Корее в Интернете РК цензурируются, все сайты КНДР заблокированы [11, с. 11]. После 2010 г. можно попасть под обвинение за положительные комментарии о КНДР в медиа [12].

Причина такого ужесточения — «DDOS-атака КНДР» 2009 г., затронувшая сайты Голубого Дома (резиденция президента РК), НАР и такие порталы, как «Naver» [13]. В 2010 г. создано «Киберподразделение национальной армии». Как утверждает РК, за одни сутки оно пресекает 90 тыс. попыток взломать сайты страны [14]. Данная структура — «противовес» Подразделению 121 из КНДР или DarkSeoulGang. С ней связывают кибератаку на Южную Корею в 2013 г. Пострадали телекомпании KBS, MBC, а также банк Woori. Адреса атакующих компьютеров были китайскими, но обвиняют КНДР [15]. Сведения о «121» противоречивы, потому ее существование под вопросом [16]. Цензурируется и медиаконтент из Японии. Его трансляция достаточно жестко ограничена в южнокорейском Интернете [17].

Второе направление — «защита нравственности». Блокируются сайты о проблемах представителей ЛГБТ-сообщества, «эротический контент», «пиратские ресурсы», сайты с азартными играми [18]. Уже в 2011 г. был запрещен доступ к более чем 53 тыс. подобного рода материалов, и это количество растет [19].

В итоге сложно сейчас назвать РК «кибербезопасной». Успехи «Киберподразделения» неубедительны. Задачи цензуры и блоки-

ровки исполняются, но сможет ли РК противостоять более опасным видам киберпреступности при их появлении в стране пока не ясно.

Литература

1. Halder D., Jaishankar K. *Cyber-crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global. 2011. 264 p.

2. 박성훈. 사이버 상에서 발생하고 있는 국제범죄의 유형과 대응방안의 모색 // 한국범죄학. 2011. 5 권 2 호. 43–80 쪽. (Пак Сонг Хун. Исследование международного вида киберпреступности в эру глобализации // Журнал Кореиск. криминолог. ассоциации. 2011. № 5–2. С. 43–80).

3. Спирина С. Г. Криминологические и уголовно-правовые проблемы в сфере компьютерной информации : дисс. ... канд. юр. наук. Краснодар, 2002. 216 с.

4. It Statistics of Korea (Ministry of Science and ICT of the Republic of Korea). URL: <http://www.itstat.go.kr/en/home.it> (дата обращения: 11.02.2019).

5. 이용환. 정보통신 기술확산의 정치경제 : 한국과 일본의 휴대전화 및 인터넷 사례비교. 서울: 연세대학교 대학원: 정치학과. 2003. 278 쪽. (Ли Ёнг Хван. Политическое и экономическое использование интернет-технологий: сравнение Японии и Кореи. Сеул: Аспирантура университета Ёнсэ: кафедра политологии. 2003. 278 с.)

6. United Nations 2018 E-government survey. URL: <https://publicadministration.un.org/egovkb/en-us/> (дата обращения: 11.02.2019).

7. 한국, 아태지역 국가 중 사이버 테러 취약성 1위. Deilotte Outlook. 24.02.2016. («РК и прочие наиболее уязвимые к кибертерроризму страны Азиатско-тихоокеанского региона», Deilotte Outlook). URL: <https://www2.deloitte.com/kr/ko/footerlinks/pressreleasespage/2016/press-release-20160224.html> (дата обращения: 13.02.2019).

8. Номоконов В. А., Тропина Н. Л. Киберпреступность как новая криминальная угроза. // Криминология: вчера, сегодня, завтра. 2012. № 1. С. 45–55.

9. 정보통신망 이용촉진 및 정보보호 등에. 24.12.2018. («Закон о содействии использованию информационно-коммуникационных сетей и защите информации»). URL: <http://www.law.go.kr/lsSc.do?menuId=0&-subMenu=1&query=정보통신망%20이용촉진%20및%20정보보호%20등>에#undefined (дата обращения: 11.02.2019).

10. 양성은. 사이버범죄의 동향고 이에 대한 형사법적 책임 // Internet & Security Focus 2013 9월호. 54–69 쪽. (Янг Сон Ён. «Тренды» современной

киберпреступности и уголовная ответственность. // Internet & Security focus. 2013. № 9. С. 54–69).

11. 신충근. 北韓의 對南 사이버테러 戰略 分析 및 對應 方案에 關한 考察. 서울: 고려대학교 대학원. 2014. 44쪽. (Син Чхунг Гын. Стратегический анализ противодействия кибер-терроризму КНДР. Сеул: аспирантура университета Корё, 2014. 44 с.)

12. 김정완. 국정원, “DDoS공격 배후, 북한과 그 추종세력으로 추정” 발표. 2009. 보안뉴스. (НАР презентует доклад, по утверждениям в котором, за DDOS-атакой может стоять КНДР и ее союзники. Боан Ньюс, 2009). URL: <https://www.boannews.com/media/view.asp?page=1&idx=16991&search=&find=&kind=1> (дата обращения: 13.02.2019).

13. 김민석 (2009년 7월 11일). “국군 사이버사령부 내년 창설 ‘인터넷 영토’ 방어 맡는다”. 중앙일보, 2009. URL: <https://news.joins.com/article/3682753> (Ким Мин Сок. 11 июля 2009 года. «Создание «киберподразделения» для защиты интернет-территорий». Чунан Ильбо, 2009) (дата обращения: 11.02.2019).

14. Kim Eun-Jung. S. Korean man indicted for pro-Pyongyang postings on Internet, Twitter. 2011. URL: <https://en.yna.co.kr/view/AEN20110110007200315> (дата обращения: 13.02.2019).

15. Tania Branigan. South Korea on alert for cyberattacks after major broadcasting network goes down. URL: <https://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack> (дата обращения: 13.02.2019).

16. Асмолов К. В. Северокорейские хакеры: нестрашная правда. РСМД, 2018. URL: <http://russiancouncil.ru/analytics-and-comments/analytics/severokoreyskie-khakery-nestrashnaya-pravda/> (дата обращения: 13.02.2019).

17. 韓流偏重批判に考慮を 自民・片山さつき議員が民放連に要請. J-cast News, 2011. (Законотворец Либерально-демократической партии Сацуки Катаяма просит «принять во внимание» политику «Халлю», одержимую критицизмом. J-cast News, 2011). URL: <http://www.j-cast.com/2011/08/31105803.html> (дата обращения: 13.02.2019).

18. Internet Censorship in South Korea. 2010. URL: <https://www.i-policy.org/2010/01/internet-censorship-in-south-korea.html> (дата обращения: 13.02.2019).

19. Choe Sang-Hun. Korea Policing the Net. Twist? It's South Korea. New York Times, 2012. URL: <https://www.nytimes.com/2012/08/13/world/asia/critics-see-south-korea-internet-curbs-as-censorship.html?pagewanted=all> (дата обращения: 13.02.2019).