МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В. ЛОМОНОСОВА

ФИЛИАЛ МГУ ИМЕНИ М.В.ЛОМОНОСОВА В Г.ЕРЕВАНЕ

Направление 41.03.05 «Международные отношения»

Выпускная квалификационная работа

Тема: «Проблема кибербезопасности как один из главных вызовов глобальной безопасности»

Исполнитель:
Студент(ка) 4 курса
Манукян Давид Норикович

Научный руководитель:
ст. преподаватель
Веселов Василий Александрович

_____
«21» 05. 2019г.

Допустить к защите

Допустить к защите:
Зам. исполнительного директора
по учебной работе
к.ф.н., доцент
Багиян Жан Григорьевич
_____
«21» 05 2019 г.

Ереван-2019

ВВЕДЕНИЕ

Актуальность темы исследования. Противодействие современным вызовам и угрозам, возникающим вследствие стремительного развития глобального информационного пространства в последние годы, является одной из основных задач, затрагивающих стратегические вопросы обеспечения стабильности современного миропорядка, решение которых возможно лишь на основе объединения усилий всех членов международного сообщества. Сложность предотвращения и сдерживания реальных и потенциальных угроз в сфере информационных технологий относится к числу наиболее значимых проблем международной и национальной безопасности XXI века.

На современном этапе мирового развития информационно-коммуникационные технологии имеют глобальное значение. Все больше документов стратегического планирования принимаются в целях обеспечения национальной безопасности в сфере информационно-коммуникационных технологий. Информационная сфера стала одной из главных составляющих жизни общества, и чем активнее она развивается, тем больше политическая, оборонная и многие другие составляющие национальной безопасности будут зависеть от кибербезопасности, а в ходе технологического развития данная зависимость будет возрастать. Уровень проникновения информационных технологий и глобальных сетей в общество напрямую связан с уровнем развития страны. Глобализация информационных отношений обусловливает мировую тенденцию к переходу противоправной деятельности в виртуальное пространство. На сегодняшний день киберпреступность, для которой не существует государственных границ, угрожает и посягает на национальные интересы и безопасность государств.

Проблема обеспечения кибербезопасности все чаще становится предметом широкой дискуссии, как на национальном, так и международном уровнях. Не в последнюю очередь это обусловлено сложным трансграничным характером проблемы и невозможностью решения значительной части задач в сфере

противодействия киберпреступникам исключительно в рамках национальных правоохранительных систем. При этом кибератаки (в различных видах) становятся повседневным контекстом деятельности государств, международных организаций и их специализированных учреждений. Концептуальная же неопределенность с формами и методами идентификации кибератак соответствии с международным законодательством, разнообразие позиций ключевых геополитических игроков, потенциальная ревизия (или просто нарушение) понятия «национальный суверенитет» обусловливает особое значение этого вопроса при исследовании проблем безопасности, которые стали актуальными с развитием информационного общества.

Степень научной разработанности темы исследования. Несмотря на широкий интерес к данному направлению безопасности, научные исследования, или даже обобщения по этому вопросу, все еще редки и часто несистемные. Так, вопросы методологии и понятийного аппарата современного киберпространства поднимались в исследованиях таких авторов, как: А.С. Алпеев[1], В.М. Елин[2], Д.А. Букин[3], Л.В. Савин[4], И.В. Авчаров[5], В.П. Харченко[6], Р. Гоутам[7], К. Вишик[8], Е.

[1] Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. - 2014. - № 5. - С. 39-42.

[2] Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: монография. - М., 2016. - 168 с.

[3] Букин Д.А. Underground киберпространства // Рынок ценных бумаг. 2013. - № 8. - С. 104 - 108.

[4] Савин Л.В. Введение в кибергеополитику // Геополитика. Информационно-аналитическое издание. Выпуск XXII, 2013. - 118 с.

[5] Авчаров И.В. Борьба с киберпреступностью // Информатизация и информационная безопасность правоохранительных органов: Сб. ст. XI межд. науч.-прак. конф. - М., 2012. - С. 191-194.

[6] Харченко В.П. Кибертерроризм на авиационном транспорте / // Проблемы информатизации и управления: Сб. науч. Трудов. Вып. 4., 2009. - С. 131-140.

[7] Goutam R. Importance of Cyber Security // International Journal of Computer Applications. - 2015 . - Vol. 7. - P. 14-17.

[8] Vishik C. Key Concepts in Cyber Security // [Electronic resource] URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch11.pdf (accessed: 23.02.2019)

Фишер[9], Д. Кофф[10], С. Солмс[11], Д. Кларк[12], Х. Менашри, Г. Барам[13], Р. Вон Солмс[14] и др.

Отдельными вопросами терминологической неопределенности предметного поля кибербезопасности занимались такие исследователи, как: К.Ф. Джаббарова[15], Кейтс А.[16], Ю.А Семенов[17], А.В. Федоров[18], В.П. Шеломенцев[19], В.А. Голубева, Э.В. Рыжкова[20], Е. Старостина[21], Дж. Аркилла, Д. Ронфельдт[22], Дж. Пандэ[23], Г. Виеманн[24] и др.

Общие вопросы правового статуса киберугроз, как на национальном, так и международном уровнях, а также вопросы, касающиеся методологического аспекта определения киберугроз, как таких, которые подпадают под понятия

---

[9] Fischer E. Cybersecurity Issues and Challenges: In Brief // [Electronic resource] URL: https://fas.org/sgp/crs/misc/R43831.pdf (accessed: 24.02.2019)

[10] Korff D. Cyber Security definitions - a selection // [Electronic resource] URL: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout%20-%20DK150119.pdf (accessed: 22.02.2019)

[11] Solms R. From information security to cyber security // Computer & Security. - 2013. - Vol 2. - P. 97-103.

[12] Clark D. Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, 12 March 2010 // [Electronic resource] URL: https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf (accessed: 27.02.2019)

[13] Menashri H., Baram G. Critical Infrastructures and their Interdependence in a Cyber Attack –The Case of the U.S. // Military and Strategic Affairs. – 2015. – Vol. 7, №. 1. – P. 99-100.

[14] Von Solms R. From information security to cyber security // Computers & security. – 2013. – Vol. 38. – P. 97–102.

[15] Джаббарова К.Ф. Современные аспекты кибербезопасности в мире в контексте глобальных угроз // АНИ: Экономика и управление. - 2017. - №. 2. - С. 323-326.

[16] Keith A. Warfighting in Cyberspace // [Electronic resource] URL: http://www.carlisle.army.mil/DIME/documents/Alexander.pdf (accessed: 01.03.2019)

[17] Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности // [Электронный ресурс] URL: http://book.itep.ru/10/2012.htm (дата обращения: 04.03.2019)

[18] Информационные вызовы национальной и международной безопасности / Под общ. ред. Федорова А.В., Цыгичко В.Н. М.: ПИР-Центр, 2001. - 328 с.

[19] Шеломенцев В.П. Концепции законопроекта о кибернетической безопасности // Борьба с Интернетпреступностью: материалы междунар. научно-техн. конф., 2013. - С. 12-14.

[20] Компьютерная преступность и кибертерроризм / под ред. В.А. Голубева, Э.В. Рыжкова. - Центр исслед. компьютерной преступности, 2005. (Вып. 3). - 448 с.

[21] Старостина Е. Терроризм и кибертерроризм — новая угроза международной безопасности // [Электронный ресурс] URL: http://www.crime-research.ru/articles/starostina/3 (дата обращения: 04.03.2019)

[22] Arquilla J., Ronfeldt D. Networks and netwars: The future of terror, crime, and militancy. Rand Corporation. 2001 // [Electronic resource] URL: https://www.rand.org/pubs/monograph_reports/MR1382.html (accessed: 06.03.2019)

[23] Pande J. Introduction to Cyber Security. - Uttarakhand Open University, 2017. - 152 p.

[24] Weimann G. Cyberterrorism: How Real is the Threat? / United States Institute of Peace Special Report 119 (2004). // [Electronic resource] URL: http://www.usip.org/publications/cyberterrorism-how-real-threat (accessed: 05.03.2019)

«применение силы» в международном законодательстве, а также вопросы международного взаимодействия по данной проблеме, посвящены работы таких исследователей, как: Л.А. Бураева[25], А.И. Згоба, Д.В. Маркелов[26], Е.С. Зиновьева[27], Дж. Фоунтеин[28], М. Либицки[29], А. Лих[30], Д. Грахам[31], А. Бэндовши[32], Н. Чоукри[33], И. Дьюк, В. Цюртила[34], Б. Геральд[35], А. Хенри[36], А. Кохен[37], Н. Руетер[38], Х Салим[39], Л. Хансен, Х. Ниссенбаум[40], Ч. Осбоум[41] и др.

---

[25] Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. - 2015. - № 13. - С. 96-99.

Бураева Л.А. Информационные войны и информационный терроризм в современном мире: методы и поле действия // Известия Кабардино-Балкарского научного центра РАН. - 2014. - № 1. - С. 7-11.

[26] Згоба А.И., Маркелов Д.В. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. - 2014. - № 5. - С. 30-38.

[27] Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы: дис. ... докт. наук: 23.00.04. - М., 2017. – 332 с.

[28] Fountain J. E. Building the virtual state: Information technology and institutional change. - Brookings Institution Press, 2001. - 256 p.

[29] Libicki M. Crisis and Escalation in Cyberspace // [Electronic resource] URL: https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf (accessed: 07.03.2019)

[30] Lih A. A virtual necessity: some modest steps toward greater cybersecurity // Bulletin of the Atomic Scientists. - 2012. - Vol. 68. - № 5. - P. 75-87.

[31] Graham D. Cyber Threats and the Law of War // Journal of National Security Law & Policy. - 2010. - Vol. 4. - P. 87-102.

[32] Bendovschi A. Cyber-Attacks – Trends, Patterns and Security Countermeasures // Procedia Economics and Finance. 2015. [Electronic resource] URL: https://www.researchgate.net/publication/283967866_Cyber-Attacks_-_Trends_Patterns_and_Security_Countermeasures (accessed: 07.03.2019)

[33] Choucri N., Goldsmith D. Lost in cyberspace: harnessing the Internet, international relations, and global security // Bulletin of the Atomic Scientists. – 2012. – Vol. 68. – P. 70-77.

[34] Duić I., Cvrtila V. International cyber security challenges // MIPRO. 2017. [Electronic resource] URL: https://bib.irb.hr/datoteka/878827.Duic_Cvrtila_Ivanjko_International_cyber_security_challenges_.pdf (accessed: 07.03.2019)

[35] Gerald B.F. The theory the intersectionality can make cyber security collaboration real // [Electronic resource] URL: https://techcrunch.com/2015/02/17/the-theory-of-intersectionality-can-make-cybersecurity-collaboration-real/ (accessed: 08.03.2019)

[36] Henry A. Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry // [Electronic resource] URL: https://unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdfRequirements (accessed: 10.03.2019)

[37] Cohen A. The Willie Sutton Theory of Cyber Security // [Electronic resource] URL: https://www.illumio.com/blog/willie-sutton-cyber-security#gsc.tab=0 (accessed: 10.03.2019)

[38] Rueter N. The Cybersecurity Dilemma. Department of political science Duke University // [Electronic resource] URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.826.7847&rep=rep1&type=pdf (accessed: 10.03.2019)

[39] Salim H. Cyber safety: A systems thinking and systems theory approach to managing cyber security risks. - Massachusetts Institute of Technology, 2014. - 157 p.

[40] Hansen L., Nissenbaum H. Digital Disaster, Cyber Security and the Copenhagen School. University of Copenhagen, New York University // International Studies Quarterly. - 2009. - № 53. - P. 1155-1175.

[41] Osborne Ch. Carbanak hacking group steal $1 billion from banks worldwide // [Electronic resource] URL: https://www.zdnet.com/article/carbanak-hacking-group-steal-1-billion-from-banks-worldwide/ (accessed: 10.03.2019)

Цель исследования – определить проблематику кибербезопасности, рассмотреть современные тенденции и обзор основных подходов ее обеспечения на международном уровне.

Данная цель определила постановку и решение следующих задач исследования:

- рассмотреть основные вопросы понимания и проблематики подходов к киберпространству;

- охарактеризовать основные аспекты и угрозы киберпезопасности в условиях современности;

- выявить ключевые вопросы обеспечения кибербезопасности на глобальном уровне;

- проанализировать усилия международных акторов и организаций в процессе обеспечения кибербезопасности.

Объект исследования – кибербезопасность как неотъемлемая часть национальной и международной безопасности.

Предмет исследования – особенности организации международного диалога по обеспечению глобальной кибербезопасности.

Методологическую основу исследования составляют как общенаучные, так и специальные методы исследования: методы анализа и синтеза, диалектический, системный, формально-юридический, конкретно-исторический и сравнительно-правовой методы исследования. Вышеуказанные методы исследования позволили получить необходимую информацию для анализа теоретических аспектов обеспечения информационной и кибербезопасности.

Структура работы включает в себя: введение, две главы, объединяющие четыре параграфа, заключение и список использованных источников и литературы.

ГЛАВА 1. ПОНЯТИЕ И КЛЮЧЕВЫЕ АСПЕКТЫ КИБЕРПРОСТРАНСТВА: УГРОЗЫ БЕЗОПАСНОСТИ

1.1. Проблематика киберпространства

Впервые термин «киберпространство» был использован в принятой представителями государств Большой восьмерки в ходе Окинавской встречи в июле 2000 г. Окинавской хартии глобального информационного общества и в Конвенции о преступности в сфере компьютерной информации от 23 ноября 2001 года[42]. Сфера его действия в то время находилась под влиянием общих механизмов правового регулирования общественных отношений, ограничиваясь специфическими объектами и интересами субъектов правоотношений, а также компьютерными сетями, с помощью которых можно участвовать в правоотношениях. В частности Окинавская хартия подтвердила роль информационно-коммуникационных технологий (далее – ИКТ) как одного из важнейших факторов, влияющих на формирование мирового сообщества в новом тысячелетии, и право каждого на возможность доступа к этим технологиям. Кроме этого, Окинавская хартия определила, что все усилия международного сообщества, направленные на построение глобального информационного общества, должны включать и действия, направленные на создание безопасного информационного пространства.

Сейчас киберпространство имеет множество определений, к примеру:

1) в соответствии с международным стандартом, киберпространство – это среда существования, возникшая в результате взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологических устройств и сетей, подключенных к ним, которого не существует в любой физической форме[43];

2) в соответствии с нормативной базой США, киберпространство – это сфера, которая характеризуется возможностью использования электронных и

[42] Окинавская хартия Глобального информационного общества от 21 июля 2000 г. // [Электронный ресурс] URL: http://www.kremlin.ru/supplement/3170 (дата обращения: 28.02.2019)
[43] ISO/IEC 27032, Information technology. Security techniques. Guidelines for cybersecurity, 2012. - 50 p.

электромагнитных средств для запоминания, изменения и обмена данными через сетевые системы и связанную с ними физическую инфраструктуру[44];

3) в соответствии с официальным документам Евросоюза, киберпространство – это виртуальное пространство, в котором циркулируют электронные данные мировых персональных компьютеров[45];

4) в соответствии с официальным документам Великобритании, киберпространство – это все формы сетевой, цифровой активности, включающие в себя контент и действия, осуществляемые через цифровые сети[46];

5) в соответствии с официальными документами Германии, киберпространство – это вся информационная инфраструктура, доступная через интернет за рамками любых территориальных границ[47].

Среди иных определений и трактовок киберпространства, стоит также отметить и такие, как:

- полиморфное виртуальное пространство, генерирующее информационные, системы как в форме сложных миров, так и в простых реализациях (наподобие электронной почты, глобальной навигации и т.д.)[48];

- коммуникационная среда, образованная системой связей между объектами киберинфраструктуры – электронными вычислительными машинами, компьютерными сетями, программным обеспечением и информационными ресурсами, используемое для обеспечения определенных информационных потребностей[49];

- искусственная электронная среда обитания информационных объектов в цифровой форме, образованная в результате функционирования кибернетических компьютерных систем управления и обработки информации,

---

[44] National Military Strategy for Cyberspace Operations // [Electronic resource] URL: http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.%20pdf (accessed: 28.02.2019)

[45] Glossary and Acronyms (Archived) / European Commission // [Electronic resource]. URL: http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c (accessed: 28.02.2019)

[46] Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space // [Electronic resource] URL: http://www.officialdocuments.gov.uk/document/cm76/7642/7642.pdf (accessed: 28.02.2019)

[47] German Cyber Security Strategy // [Electronic resource] URL: http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy2011-1 (accessed: 28.02.2019)

[48] Харченко В.П. Кибертерроризм на авиационном транспорте / // Проблемы информатизации и управления: Сб. науч. Трудов. Вып. 4., 2009. С. 133.

[49] Goutam R. Importance of Cyber Security // International Journal of Computer Applications. - 2015 . - Vol. 7. P. 15.

которая способна обеспечивать пользователям непосредственный доступ к вычислительным и информационным ресурсам систем, выработку электронных информационных продуктов, а также обмен электронными сообщениями, давая возможность с применением электронных информационных образов в режиме реального времени вступать в отношения (взаимодействовать) по совместному использованию вычислительных и информационных ресурсов системы (предоставление информационных услуг, ведение электронной коммерции и т.д.)[50];

- пространство, сформированное информационно-коммуникационными системами, в котором происходят процессы преобразования (создание, хранение, обмена, обработки и уничтожения) информации, представленной в виде электронных компьютерных данных[51];

- объекты информационной инфраструктуры управляемые информационными (автоматизированными) системами управления и циркулирующей в таковых информации[52];

- среда, образованная организованной совокупностью информационных процессов на основе объединенных по единым принципам и правилам информационных, телекоммуникационных и информационно-телекоммуникационных систем[53].

Исходя из вышеизложенного, наиболее отличительными признаками киберпространства как субстанции, созданию которой способствовали, прежде всего, следующие факторы: изменение характера деятельности человека по принятию решений; внедрение электронно-цифровых форм создания, обработки, хранения и перемещения информации, переход от бумажного делопроизводства к электронному т.д.[54], – абсолютное большинство

---

[50] Vishik C. Key Concepts in Cyber Security // [Electronic resource] URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch11.pdf (accessed: 23.02.2019)

[51] Fischer E. Cybersecurity Issues and Challenges: In Brief // [Electronic resource] URL: https://fas.org/sgp/crs/misc/R43831.pdf (accessed: 24.02.2019)

[52] Korff D. Cyber Security definitions - a selection // [Electronic resource] URL: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout%20-%20DK150119.pdf (accessed: 22.02.2019)

[53] Solms R. From information security to cyber security // Computer & Security. - 2013. - Vol 2. P. 101.

[54] Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. - 2014. - № 5. С. 41.

исследователей считает его непревзойденные возможности по созданию бессчетных связей между отдельными индивидами и социальными группами и по предоставлению разноплановых информационных услуг[55].

Учитывая вышеизложенное, считаем целесообразным понимать под киберпространством виртуальную коммуникационную среду, образованную системой связей между пользователями и объектами информационной инфраструктуры, такими как электронный информационный ресурс, системы и сети всех форм собственности, управляемые автоматизированными системами управления, которые используются не только для преобразования и передачи информации, которая в них циркулирует, с целью обеспечения информационных потребностей общества, но и для влияния на аналогичные объекты противоборствующей стороны.

Исходя из этого вполне закономерной видится ситуация в рамках которой в отечественных и научных кругах встречаются мнения исследователей, связанные с возрастающим значении киберпространства в качестве непосредственного инструмента политики, тогда как само киберпространство является «полем где разворачивается противоборство политических организаций, стран и альянсов государств»[56]. В данном контексте также стоит отметить, что инциденты с Э. Сноуденом и Д. Ассанджем является показательным фактом того, как именно коммуникации, связь социальной среды с политикой, военным сектором, экономикой влияют на позиции отдельных, ведущих стран мира[57]. Фактически, за право влияния в киберпространстве на сегодняшний день ведется активная борьба между разными международными акторами, прикладывающими не только существенные усилия в виде создания специальных подразделений в рамках государственных органов, в сферу ответственности которых входит мониторинг и формирование общественного мнения в интернете по тому или иному вопросу, но и в достаточно больших

[55] Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: монография. - М., 2016. С. 23.
[56] Букин Д.А. Underground киберпространства // Рынок ценных бумаг. 2013. - № 8. С. 105.
[57] Савин Л.В. Введение в кибергеополитику // Геополитика. Информационно-аналитическое издание. Выпуск XXII, 2013. С. 5.

бюджетных вливаниях в развитие технологий и формирование новых инструментов в данном направлении.

Кроме этого, в своей практической плоскости являются достаточно заметными и отличия в подходах государств к восприятию киберпространства как такового – так, такие страны как США, Великобритания, Франция, Германия, Италия, Испания, иные страны Запада в подавляющем своем большинстве продвигают тезис о свободе действий в Интернете, хоть и с некоторыми оговорками в виде противодействия терроризму, противодействию их последователям и т.д., тогда как Российская Федерация, Украина, Беларусь, Иран, Китай, Индия, иные страны продвигают тезис о том, что Интернет должен функционировать под юрисдикцией норм международного права (Международного Союза Электросвязи, который входит в ООН). В данном контексте стоит отметить, что Саммит по вопросам киберпространства, который прошел в Дубаи в 2012 году, также продемонстрировал наличие различных точек зрения, связанных с будущим и развитием киберпространства у различных государств, включая демонстрацию противоречий, связанных с международными телекоммуникациями – особо явно данный тезис проявился в том, что Соединенные Штаты отказались от подписания договора, регламентирующего право государств на управление Интернетом[58].

В данном контексте, важно понимать, что киберпространство отличается от «традиционного» наземного, воздушного, морского, космического пространства тем аспектом, что киберпространство создано не природой, а является целиком искусственной конструкцией, в систему которой включены компоненты, которые по прошествии времени могут трансформироваться и обретать новые формы и направления взаимодействия.

В своей совокупности, адекватное и стабильное функционирование киберпространства имеет ключевое значение для экономики, национальной безопасности любого государства. Также важно отметить, что

[58] Авчаров И.В. Борьба с киберпреступностью // Информатизация и информационная безопасность правоохранительных органов: Сб. ст. XI межд. науч.-прак. конф. - М., 2012. С. 192.

киберпространство достаточно тесно связано с географией, которая является одновременно с политикой одним из главных элементов геополитических процессов, протекающих сегодня в мире. Во многом, данное обстоятельство связано с тем, что маршруты коммуникаций, сервера, различных технические узлы, на которых и «базируется Интернет», имеют свою географическую локализацию. Кроме этого, киберзоны имеют национальную идентификацию, что проявляется в наличии отдельных доменных зон, языка, определенного государственного контроля – фактически, киберпространство демонстрирует физическую географию своим характерным образом, что проявляется в системной работе датчиков служб, навигационных устройств, гаджетов и мобильных устройств, в которых учитываются текущие потоки информации в целом.

Применимо к основным каналам информации стоит отметить, что основной информационный трафик идет по различным подводным кабелям, связывающим на сегодняшний день все континенты[59]. Кроме этого, государства могут нести прямую ответственность за события которые происходят в киберпространстве, учитывая тот факт, что физические маршруты коммуникаций могут проходить через национальные территории того или иного государства. Также важным фактором для современной геополитики связан с глобальностью – так, киберпространство последовательно фиксирует, гомогенизирует физическое пространство с помощью технологии GPS, иных инструментов, что позволяет процессам глобализации в качестве явления охватывать фактически все уголки планеты. Исходя из этого возможным видится допущение том, что картографирование Интернет-пространства является приоритетной задачей для профильных исследовательских центров и университетов, в результате чего с каждым годом появляются новые специализированные направления работы в данной плоскости, осуществляется более всесторонний мониторинг киберпространства с фиксацией характерных

[59] Антонос Г. А. Международные изменения права киберпространства // Право и информатизация общества: сб. науч. тр. - М.: ИНИОНРАН, 2012. С. 177.

изменений в данной плоскости – появления новых технических узлов, издания новых законопроектов в отдельных государствах, либо противоправная деятельности в сети в целом.

Исходя из этого не представляется возможным в рамках данной работы допустит тезис о том, что современное киберпространство является однородным – в данном случае, уместно сделать допущение о том, что на современном этапе киберпространство является неоднородным, имеющим несколько достаточно характерных уровней. Так. По мнению Д. Кларка, модель киберпространства включает в себя четыре характерных уровня:

1. Физический уровень киберпространства – данный уровень включает в себя аппаратные устройства, переключатели, носители, маршрутизаторы, спутники, датчики, различные соединители (подводные, беспроводные) – иными словами, физическая инфраструктура расположена в физическом пространстве и, как результат, физическая инфраструктура является предметом различных национальных юрисдикций;

2.Логический уровень киберпространства – программный код, скрипты, включающие программное обеспечение, запускающее характерные протоколы, которые включены в код;

3.Уровень контента киберпространства – созданная информация, обрабатываемая информация, поступающая информация, исходящая информация, хранящаяся информация, воспроизводимая и иная информация, которая транслируется, воссоздается, передается в рамках киберпространства и представляет собой знания, факты, события, вещи, компоненты, процессы либо идеи;

4.Социальный уровень киберпространства – люди, формирующие и использующие киберпространство – «Интернет людей», потенциальные отношения, взаимосвязи между людьми с помощью киберпространства[60].

[60] Clark D. Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, 12 March 2010 // [Electronic resource] URL: https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf (accessed: 27.02.2019)

В данном контексте стоит отметить, что социальная плоскость включает в себя и правительство, и частный сектор и гражданское, техническое сообщество – каждая из данных категорий объединена с другими категориями общей спецификой – если в физическом плане, граждане могут быть идентифицированы, к примеру, по отпечаткам пальцев либо ДНК, то подобная идентификация в сети является более сложным и многогранным явлением – в отличие от реального мира, люди в киберпространстве имеют возможность создания множественной идентичности для пользователя – иными словами, виртуальная личность может иметь сразу несколько реальных пользователей, что важно с точки зрения защиты безопасности, авторских прав и поднимает вопросы о том, какую роль данное пространство играет в реальном мире[61].

В данном контексте необходимо отметить, что в своей совокупности киберпространство включает в себя и физические основы (кабеля, вышки связи, компьютеры, маршрутизаторы, сервера), логический уровень (протоколы, программное обеспечение, браузеры, систему доменных имен), информационный слой (текст, видео, фотографии, иные материалы которые преобразуются, передаются, Хранятся в киберпространстве), пользователей (люди, субъекты, формирующие киберопыт, природу киберпространстве в процессе работы с информацией).

В своей системе, каждый последующий уровень непосредственно связан с доступными и осуществляемыми функциями на предыдущих уровнях. Кроме того, указанная модель представляет полезное устройство для определения местонахождения субъектов, видов их деятельности в данном пространстве, в том числе, позволяет выявлять технологические изменения, определять условия, при которых субъекты действуют на разных уровнях, позволяет отслеживать закономерности и зависимости, влияние тех или иных факторов на структуру киберпространства.

[61] Tackling the Challenges of Cyber Security / ETSI White Paper No. 18. December 2016 [Electronic resource] URL: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp18_CyberSecurity_Ed1_FINAL.pdf (accessed: 27.02.2019)

В данном контексте, общий способ оценки структуры и процесса непосредственно в международных отношениях, сводится к концентрации внимания на уровнях анализа, которые включают в себя непосредственно индивида, государства, международную систему. Данная иерархия базируется на принципе суверенитета, который проводит различие между непосредственно государством, иными субъектами, что позволяет обеспечить правовую основу для современной системы международных отношений. Также ряд исследователей выделяют дополнительный уровень – «всеобъемлющую глобальную систему»[62].

На базе данной модели в рамках данной работы становится реальным определение характерных последствий, связанных с использованием, функционированием и формированием киберпространства в целом. Так, кибердоступ расширяет возможности человека, тогда как само киберпространство предоставляет новые способы формирования, объединения интересов человека, позволяет мобилизовать усилия людей, сконцентрировать внимание общества на определенных фактах, явлениях и т.д. Иными словами, индивид получает возможность «иметь значение» в государственной суверенной системе международных отношений. В дальнейшем, построение киберпространства создает новые возможности для формирования новых систем связанных с пониманием и измерением, обеспечением безопасности государства, что, с одной стороны усложняет формирование новых структур безопасности, которая в своем традиционном значении опирается на внешнюю безопасность (защита от военных угроз) и включает в сея внутреннюю безопасность (стабильность, легитимность управления), экологическую безопасность (устойчивость жизнеобеспечивающих свойств природы).

В данном контексте стоит отметить, что на данный момент общество сталкивается с фактом возрастающих угроз кибербезопасности, что проявляется с угрозой для безопасности информации, знаний в интернете, защите от

[62] Menashri H., Baram G. Critical Infrastructures and their Interdependence in a Cyber Attack –The Case of the U.S. // Military and Strategic Affairs. – 2015. – Vol. 7, №. 1. – P. 99-100.

киберугроз, противодействия шпионажу, саботажа, противодействие росту преступности и мошенничества в интернете, что делает вопрос кибербезопасности важным вопросом как в национальном, так и в международном контексте.

Также стоит отметить, что в современных условиях международная система включает в себя как отдельные суверенные государства, так и негосударственные субъекты, которые обычно рассматриваются в качестве транснациональных субъектов, действующих за рамками одного государства и имеющих корни в различных государствах[63].

В данном контексте, киберпространство помогает более полно сформировать новые частные интересы, что позволяет сформировать новые субъекты с характерными целями, приоритетами, задачами и проблемами. Также киберпространство является новым полем для конфликтов, разногласий, взаимодействия между государствами, принимающими участие в данном киберпространстве.

1.2. Основные аспекты кибербезопасности

На современном этапе, важность киберпространства подтверждается появлением концепций ведения борьбы в нем и созданием в составе вооруженных сил многих стран мира специальных структур, наподобие:

- Объединенного киберкомандования и специализированного кибернетического разведывательного центра в США;
- Управления сетевых операций в Германии;
- Центрального управления по кибербезопасности, оперативного центра обеспечения кибербезопасности (CSOC) и Центра государственного связи в Великобритании;

[63] Digital Europe: Pushing the frontier, capturing the benefits / McKinsey Global Institute. June 2016 [Electronic resource] URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20europe%20pushing%20the%20frontier%20capturing%20the%20benefits/digital-europe-full-report-june-2016.ashx (accessed: 01.03.2019)

- Центра информационных систем Службы безопасности и Национального агентства безопасности информационных систем во Франции;

- Специализированного центра защиты национального киберпространства «Tehila» в Израиле;

- Киберподразделения в составе Федеральной службы безопасности Российской Федерации и др[64].

В целом, все приведенные центры и подразделения предназначены для ведения, так называемой, киберборьбы в качестве комплекса мероприятий, направленных на осуществление управленческого или деструктивного влияния на автоматизированные ИТ-системы противоборствующей стороны и защиты от такого воздействия собственных информационно-вычислительных ресурсов благодаря использованию специально разработанных программно-аппаратных средств, а также проведению системы специализированных учений[65].

Такое положение вещей вызывает невиданные доселе глубинные изменения в отношении большинства государств мира к безопасности собственного информационного и киберпространства, а, следовательно, постепенно приводит к необходимости усиленной защиты информации, средств ее обработки и киберсреды, в котором эта информация циркулирует, то есть – к принятию мер по обеспечению информационной и кибербезопасности.

При этом информационную безопасность в самом общем смысле можно определить как такое состояние защищенности информационного пространства государства, при котором невозможно нанести ущерб свойствам объектов безопасности, касающихся информации и информационной инфраструктуры, и который гарантирует беспрепятственное формирование, использование и развитие национальной информационной сферы в интересах обороны.

Кибербезопасность при этом можно определить как состояние защищенности киберпространства государства в целом или отдельных объектов

---

[64] Бурячок В.Л. Информационная и кибербезопасность: социотехнические аспект: учебник / под общ. ред. В.Б. Толубко. - К.: ДУТ, 2015. С. 13.

[65] Keith A. Warfighting in Cyberspace // [Electronic resource] URL: http://www.carlisle.army.mil/DIME/documents/Alexander.pdf (accessed: 01.03.2019)

ее инфраструктуры от риска постороннего кибервлияния, при котором обеспечивается их устойчивое развитие, а также своевременное выявление, предотвращение и нейтрализация реальных и потенциальных вызовов, кибернетических вмешательств и угроз личной, корпоративным или национальным интересам[66].

С развитием ИКТ, ИТС и глобальной сети Интернет мировое сообщество, получив невиданные доселе возможности в плане обмена информацией, стало чрезвычайно уязвимым из-за стороннего кибернетического воздействия, а именно в отношении фактически нескрываемых попыток влияния противоборствующих сторон на информационное и киберпространства друг друга за счет использования средств современной вычислительной или специальной техники и соответствующего программного обеспечения – кибервмешательств, а также других проявлений их дестабилизирующего воздействия на тот или иной объект, совершаемого за счет технологических возможностей информационного и киберпространства, с созданием опасности – так называемых киберугроз, как для этого пространства, так и для сознания каждого человека.

В данном контексте, во избежание многозначности толкований соответствующих терминов инструктивные материалы Интерпола разделяют их на группы, включающие:

- непосредственно компьютерные инциденты, которые заключаются, например, во вмешательстве в работу вычислительных систем, нарушении авторских прав на программное обеспечение, а также в хищении данных;

- инциденты, связанные с компьютерными системами, сопровождающих в основном противоправные действия по финансовому мошенничеству;

- сетевые инциденты, приводящие к заключению незаконных сделок[67].

[66] GAO-10-628. Key Private and Public Cyber Expectations Need to Be Consistently Addressed / United States Government Accountability Office, Washington, July 2010 // [Electronic resource] URL: https://www.gao.gov/assets/310/307222.pdf (accessed: 02.03.2019)

[67] Cyberspace. United States Faces Challenges in Addressing Global Cybersecurity and Governance / Washington, July 2010 // [Electronic resource] URL: https://www.gao.gov/assets/310/308401.pdf (accessed: 02.03.2019)

Отметим, что интерес в плане классификации кибернетических вмешательств и угроз составляет схема, предложенная Конвенцией Совета Европы 2001 года и направленной на борьбу с киберпреступностью[68]. В ней говорится о четырех возможных группах следующих действий:

1. Инциденты, ставящие своей целью нанести ущерб конфиденциальности, целостности и доступности компьютерных данных и систем, реализуемые через:

- несанкционированный доступ в информационную среду;

- вмешательство в данные (противоправное изменение, повреждение, удаление, искажение или блокирование компьютерных данных и управляющих команд с помощью кибератак на информационные системы, ресурсы и сети государственного и военного управления);

- вмешательство в работу системы;

- незаконный перехват (противоправный умышленный перехват не предназначенных для общего доступа компьютерных данных, передаваемых в обход мер безопасности);

- незаконное использование компьютерного и телекоммуникационного оборудования.

2. Мошенничество и подделка, связанные с использованием компьютеров, а именно:

- подделка документов с применением компьютерных средств (противоправное умышленное внесение, изменение, удаление или блокирование компьютерных данных, что приводит к снижению достоверности документов)

- мошенничество с применением компьютерных средств (вмешательство в функционирование компьютерной системы с целью умышленного противоправного получения экономической выгоды).

3. Инциденты, связанные с размещением в сетях противоправной информации (в частности фактор даркнета, связанный с распространением преступного контента, к примеру, наркотических веществ, детской

[68] Convention on Cybercrime. Budapest, 23 November 2001 // [Electronic resource] URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (accessed: 02.03.2019)

порнографии). В данном контексте необходимо отметить, что в силу глобализации, технологии равно как информационный прогресс в целом, позволяют правоохранительным органам создавать новые инструменты противодействия преступности, тогда как преступники получают, в силу развития новых технологий, новые способы уклонения от ответственности и формирования новых преступных схем, сообществ, направлений преступной деятельности. Производители нелегального товара, лица ответственные за сбыт, курьеры, экстремисты, иные криминальные элементы могут укрываться от органов следствия в информационном пространства в различных «скрытых от общих глаз» ресурсах, именуемых «Даркнет». Исходя из этого, данный «Теневой интернет» получает репутацию доли информационного пространства, в рамках которого возможна покупка различных запрещенных законодательствами многих стран товаров – отдельных видов порнографии, оружия, психотропных веществ, специфических услуг вроде киллеров, баз данных, паспортных данных, пластиковых карт, взрывчатых веществ, тогда как оплата осуществляется преимущественно теми или иными видами криптовалют[69]. Характеризуя конкретные угрозы, которые может представлять собой «Теневой интернет», в рамках данной работы следует отметить следующие направления:

1. Дестабизация экономики того или иного государства, по причине наличия множества площадок, позволяющим правонарушителями анонимизировать полученные криминальным способом средства, включая уклонение от уплаты налогов;

2. Формирование благоприятных условий для формирования, развития экстремистских настроений, координации действий экстремисткой направленности, что является угрозой экономической, политической и региональной безопасности;

3. Угроза личной безопасности граждан – в силу того обстоятельства, что в «Даркнет» представлен широкий диапазон различных услуг, товаров – от

[69] Галий А.А. Слюсарь И.В. «Даркнет» как угроза национальной безопасности Российской Федерации // Вестник науки. - 2018. - № 9. С. 204.

наркотиков, до боеприпасов, оружия, поддельных документов, комплектующих для их изготовления, покупка которых возможна на различных тематических площадках;

4. Угроза военной безопасности государства, угрозы территориальной целостности – в силу доступности вооружения на данных ресурсах и в силу вероятности их покупки для оснащения большого количества боевиков различных экстремистских организаций для осуществления противоправных действий на территории определенных государств:

5. Угроза безопасности личного имущества – по причине большой концентрации специалистов по «кардингу» – мошенников, специализирующихся на получении реквизитов, данных кредитных карт для получения средств того или иного человека;

6. Угроза информационной безопасности физических, юридических лиц, информационной безопасности в целом, включая тягу молодого поколения к запрещенным ресурсам, что облегчает вербовку новых боевиков и активизирует формирование экстремистских настроений. Кроме того, в государственном масштабе угрозу представляют разработки различных вирусов-шифровальщиков, эксплуатация уязвимостей государственного программного обеспечения, компрометация учетных данных, незаконное получение доступа к государственным ресурсам, что представляет опасность для обеспечения информационной, национальной безопасности для фактически любого государства[70].

На базе данных тезисов стоит отметить, что «Даркнет» является как источников угрозы, так и источником концентрации преступных элементов, мошенников и террористов, в том числе, является источником для вербовки и формирования экстремистских настроений, и включает в себя большое количество площадок для торговли запрещенными товарами (оружие,

[70] Robertson J., Diab A. Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence // FALL. 2016. [Electronic resource] URL: https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Darknet_Mining_and_Game_Theory_Robertson_et_al.pdf?ver=2018-08-01-090210-620(accessed: 22.03.2019)

боеприпасы, наркотики, психотропные и иные вещества), что делает «Даркнет» в целом опасным как для отдельных личностей, так и для общества, государства и национальной, информационной безопасности в целом, в результате чего уполномоченных органы прикладывают усилия для снижения указанной опасности на региональном, глобальном уровне, однако в рамках данной работы стоит отметить, что полное ограничение доступа пользователей в данный сегмент интернета не представляется, по мнению экспертов, возможным по техническим причинам, однако данная деятельность осуществляется с помощью модернизации информационной инфраструктуры, модернизации методов противодействия данным элементам, как на частном, так и на государственном уровне, с целью минимизации данных проявлений и угроз для национальной и информационной безопасности государства.

Исходя из такого разнообразия и скрытых возможностей, деструктивные инциденты в сфере высоких технологий в странах мира стремительно приближаются к значительным масштабам, их число неуклонно увеличивается. В частности, только за период с 2002-го по 2010 год количество раскрытых внутренних и внешних инцидентов возросло примерно в 2,5 раза[71]. За последнее десятилетие масштабные кибератаки набирают свои обороты, чему, в частности, является подтверждением: кибератака перед саммитом «Большой двадцатки» в Париже в 2010г., первая межконтинентальная кибератака Stuxnet в Иране 2010 г., в результате которой были поражены автоматизированные системы управления инфраструктурой страны; утечка данных в результате кибератаки на серверы Пентагона в 2011 г. и кибератаки серверы «Банка Америки» того же года, с последующей публикацией конфиденциальной информации в сети Интернет[72]; кибератаки в 2012 г. на сайты государственных учреждений Израиля (армии и спецслужб), а также мощная кибератака на Министерство обороны

[71] Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности // [Электронный ресурс] URL: http://book.itep.ru/10/2012.htm (дата обращения: 04.03.2019)
[72] Супертерроризм: новый вызов нового века / Научный записки ПИР-Центра // Под общей редакцией Федорова А.В. - М. : Изд-во «Права человека», 2002. С. 95.

Швеции того же года; в 2013 г. с помощью DDoS-атаки был выведен из строя официальный сайт Агентства национальной безопасности США и др[73].

Исходя из вышеуказанного, можно говорить о том, что преступные действия по организации различного рода кибератак, несанкционированного доступа к чужим сайтов, создание «сайтов-двойников» вышли за пределы отдельных стран, причем по темпам роста значительно опережают остальные виды организованной преступности[74]. Более того, в последние годы они получили существенную финансовую поддержку и высококачественные коммуникации, охватив все виды преступлений, совершенных в ИТ-сфере[75]. Однако до сих пор нет четкого определения соответствующих понятий, в том числе и такого понятия, как кибератака. Учитывая это, проанализируем известные подходы к его толкованию. Так, например, В. Харченко определяет кибератаки как мероприятия, осуществляемые для подрыва безопасности систем или реализации угрозы характеристикам безопасности ресурсам информационных систем, из-за использования уязвимостей[76]. Д. Дубов и М. Ожеван квалифицируют кибератаки как целенаправленные действия, реализуемых в киберпространстве (или с помощью технических возможностей этого пространства), которые приводят (могут привести) к достижению несанкционированных целей (нарушение конфиденциальности, целостности, авторства, доступности информации, деструктивных информационно-психологических воздействий на сознание и психическое состояние людей)[77]. В. Шеломенцев под кибератаками понимает процесс реализации программно-математических мер, направленных на поиск и использование кибернетических уязвимостей информационных, телекоммуникационных и информационно-телекоммуникационных систем[78]. Э.В. Рыжкова рассматривает кибератаки, как

[73] Pande J. Introduction to Cyber Security. - Uttarakhand Open University, 2017. P. 40-41.
[74] Информационные вызовы национальной и международной безопасности / Под общ. ред. Федорова А.В. и Цыгичко В.Н. М.: ПИР-Центр, 2001. С. 98.
[75] Arquilla J., Ronfeldt D. Networks and netwars: The future of terror, crime, and militancy. Rand Corporation. 2001 // [Electronic resource] URL: https://www.rand.org/pubs/monograph_reports/MR1382.html (accessed: 06.03.2019)
[76] Харченко В.П. Указ. Соч. С. 134.
[77] Дубов Д.В., Ожеван М.А. Кибербезопасность: мировые тенденции и вызовы. - К.: НИСИ, 2011. С. 8.
[78] Шеломенцев В.П. Концепции законопроекта о кибернетической безопасности // Борьба с Интернетпреступностью: материалы междунар. научно-техн. конф., 2013. С. 13.

результат использования технических недостатков механизмов безопасности современного киберпространства с целью дезорганизации работы его элементов[79].

Обобщая вышесказанное, можно сформулировать следующее определение: кибератака – совокупность согласованных по цели, содержанию и времени действий или мероприятий – так называемых киберакций, направленных на определенный объект воздействия с целью нарушения конфиденциальности, целостности, доступности, наблюдаемости и авторства информации, циркулирующей в нем, с учетом ее уязвимости, а также нарушения работы ИТ-систем и сетей конкретного объекта.

В последнее время сложность кибератак, а также их количество и частота постепенно растут. Своего апогея они достигли в настоящее время в глобальной сети Интернет, которая со временем начала влиять на развитие всей планеты и стала незаменимым депозитарием общечеловеческого знания. Сегодня интернет может быть, как предметом (целью) преступных посягательств, так и средой, в которой совершаются правонарушения[80]. По заключению экспертов исследовательского института United States Institute for Peace (USIP), именно сеть Интернет представляет собой «идеальную среду для деятельности террористов, ведь доступ к этой глобальной сети слишком легкий, в ней очень легко обеспечить анонимность пользователей, она никем не управляется и не контролируется , в ней не действуют законы и не существует полиции»[81].

Подтверждением такого вывода стали результаты исследований Institute for Security Technology Studies At Dartmouth College (США) ставящих своей целью прогнозирование ситуации в сети Интернет вследствие осуществления США широкомасштабной антитеррористической кампании после трагедии 11 сентября 2001 года. В отчете под названием «Cyber Attacks During The War on

[79] Компьютерная преступность и кибертерроризм / под ред. В.А. Голубева, Э.В. Рыжкова. - Центр исслед. компьютерной преступности, 2005. (Вып. 3). С. 116.
[80] Старостина Е. Терроризм и кибертерроризм — новая угроза международной безопасности // [Электронный ресурс] URL: http://www.crime-research.ru/articles/starostina/3 (дата обращения: 04.03.2019)
[81] Weimann G. Cyberterrorism: How Real is the Threat? / United States Institute of Peace Special Report 119 (2004). // [Electronic resource] URL: http://www.usip.org/publications/cyberterrorism-how-real-threat (accessed: 05.03.2019)

Terrorism: A Predictive Analysis», опубликованном 22 сентября 2001 г., специалисты института проанализировали политические конфликты, которые стимулировали рост количества атак на ресурсы сети Интернет. Речь шла, в частности, о конфликтах между Индией и Пакистаном, Израилем и Палестиной, НАТО и Сербией, США и Китаем. Специалисты института констатировали, что физические атаки на элементы критически важной инфраструктуры ведущих стран мира сопровождаются непременным ростом числа кибератак, прежде всего на серверы и активное сетевое оборудование, подключенное к этой глобальной сети[82].

Представители института System Administrator and Network Security (США) и Центра по защите национальной инфраструктуры при ФБР сделали совместное заявление о том, что осуществление кибератак становится мощным средством ведения информационных войн между государствами, а сеть Интернет – незаменимым инструментом киберпланирования, которая обеспечивает современным террористам анонимность, возможность управлять и координировать действия при подготовке и осуществлении терактов.

Характеризуя же киберпространство в качестве непосредственной сферы противоборства, в рамках данной работы необходимо отметить, что большинство существующих систем взаимодействия и передачи информации в различных странах базируются на компьютерных технологиях и различных информационных инфраструктурах и с каждым годом данная возрастающая зависимость от указанных технологий предполагает, что в случае нанесения информационного удара по данным процессам, указанное действие может нарушить либо полностью парализовать основные системы обеспечения передачи информация и обеспечения безопасности того или иного государства, либо целого региона.

В данном контексте, информационные возможности, глобальное распространение информационных технологий могут представлять для

[82] Cyber Attacks During The War on Terrorism: A Predictive Analysis September 22, 2001 // [Electronic resource] URL: http://www.ists.dartmouth.edu/docs/cyber_a1.pdf (accessed: 05.03.2019)

государств опасность, в особенности, в плоскости киберпространства, которая может, в свою очередь исходить от различных элементов, враждебных стран, террористических организаций, отдельных преступных элементов, отдельных лиц, которые руководствуются своими личными целями. Фактически, данная угроза является достаточно актуальной и в силу того фактора, что управление, функции контроля существующими системами безопасности, работа данных систем в целом, может быть нарушения в силу характерных изменения в протоколах, компьютерных программах, что позволит нанести существенный урон обороноспособности государства, стабильности государства без нанесения непосредственных физических атак и без физического уничтожения той или иной сопутствующей информационной инфраструктуры[83].

Стоит понимать, что сила любого суверенного государства прямо зависит от экономического, научного, общественного потенциала, что сопровождается наличием военной силы, задача которой сводится к защите территории государства, граждан государства от любых внешних угроз и с целью поддержки экономической, социальной, политической стабильности государства.

Уязвимость информационной инфраструктуры, систем коммуникации может привести к изменению концепции национальной обороны и защиты государства – иными словами, национальная экономика, экономические и гражданские системы могут быть подвержены опасности без прямого использования огневой мощи либо каких-то военных действий.

Исходя из этого, способность государств действовать в киберпространстве в контексте оборонительных и наступательных действиях, во многом связана с классическими военными возможностями, играющими важную роль для обеспечения безопасности современного государства.

Как результат, уже продолжительное время для многих государств киберпространство является непосредственной областью стратегического значения, и данному фактору есть сразу несколько причин:

[83] Джаббарова К.Ф. Современные аспекты кибербезопасности в мире в контексте глобальных угроз // АНИ: Экономика и управление. - 2017. - №. 2. С. 324.

1.Угроза кибератак является одной из основных угроз и рисков для национальной безопасности фактически любого государства;

2.Информационное противодействие терроризму в киберпространстве является важным направлением деятельности для США, стран Запада, РФ, Китая, Индии, иных стран[84].

Также возрастает роль киберпространства в качестве основного поля противодействия между различными геополитическими оппонентами, в силу того факта, что использование киберпространства требует сравнительно меньших ресурсов, по сравнению с формированием сопоставимой с крупными государствами военной мощи, однако информационное противодействие, в свою очередь, при определенных условиях, может нанести схожий урон. Тем не менее, относительная простота использования информационного пространства, приводит к тому, что современные крупнейшие геополитические акторы, кроме непосредственного информационного противодействия с сопоставимыми оппонентами, должны учитывать вероятность враждебных действий со стороны более мелких участников в информационном пространстве – террористических организаций, отдельных экстремистов и т.д. В контексте данных угроз, как было отмечено ранее, в большинстве стран мира были созданы специальные органы для противодействия в киберпространстве включая защиту стратегических объектов информационной инфраструктуры[85].

На сегодняшний день, существует пять основных групп, которые используют, либо имеет потенциал для фактического использования кибератак с помощью характерных инструментов:

1.Государства, выделяющие достаточные средства на защиту информационной инфраструктуры, в том числе, развивающие данное направление в контексте развития своих наступательных и оборонительных возможностей в рамках каждого отдельного государства;

---

[84] Fountain J. E. Building the virtual state: Information technology and institutional change. - Brookings Institution Press, 2001. P. 147.

[85] Libicki M. Crisis and Escalation in Cyberspace // [Electronic resource] URL: https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf (accessed: 07.03.2019)

2.Преступные элементы – во многом, деятельность данной категории связана с незаконной деятельностью в сфере коммерческих интересов (коммерческий шпионаж, и т.д.):

3.Коммерческие корпорации, заинтересованные в уничтожении, дискредитации своих конкурентов;

4.Террористические организации, осуществляющие в информационном пространстве деятельность, направленную на устрашение, запугивание населения, включая различные кибератаки на правительственные системы обеспечения безопасности, жизнедеятельности общества;

5.Анархисты, выступающие против существующих элит и которые заинтересованы в уничтожении тех или иных политических элит, использующие компьютерные системы для воздействия на различные правительственные структуры.

В данном контексте следует понимать что фактически киберперступность как и любой другой элемент свойственный воздействию одного актора на другого актора может существенным образом в долгосрочной перспективе изменить баланс сил в обществе, учитывая тот факт, что киберперступность дает возможность сторонам принимающим участие в ассиметричных конфликтах, использовать в максимальной степени доступные ресурсы для осуществления своего противодействия[86] – иными словами, возможности в данной сфере позволяют террористическим организациям, не обладающим, по сравнению с государством, существенными ресурсами, осуществлять системные атаки на наиболее важные точки обеспечения жизнедеятельности и безопасности государства, нанося при этом реальный ущерб и оказывая психологическое воздействие на общество, которое подверглось нападению в целом.

Получается, террористические группировки и отдельные лица, располагаясь в киберпространстве обладают возможностями, которые отличаются от традиционных возможностей и инструментов, отличных от

[86] Lih A. A virtual necessity: some modest steps toward greater cybersecurity // Bulletin of the Atomic Scientists. - 2012. - Vol. 68. - № 5. P. 81.

традиционных террористических инструментов, связанных с физическим воздействием и насилием[87].

Кроме этого, киберпреступления являются предпочтительными для современных преступников и террористических группировок в связи с определенными «преимуществами», вытекающими из сущности данного явления – к примеру, киберпреступление в большинстве своих проявлений не требует наличия исполнителя физически возле инфраструктуры на которую совершается атака – иными словами, возможность осуществления дистанционных атак при которых исполнитель будет находиться в любой точке земного шара предполагает анонимность и безопасность исполнителя, однако при сопоставимом с физическим уничтожением уроном для информационной инфраструктуры. Учитывая тот факт, что кибератаки происходят не в физическом пространстве. А несут в себе потенциал для серьезного ущерба в информационной сфере, данное воздействие может являться не только производным инструментом, в сравнении с традиционным физическим воздействием, но и самостоятельным направлением деятельности для террористических организаций и отдельных лиц. Исходя из этого, даже если большинство террористических атак являются ограниченными во времени и пространстве, то кибератаки могут иметь расширенные границы как во времени, так и по охвату населения, при этом нести схожие с традиционными террористическими атаками функции – психологическое воздействие на оппонента, вселение чувства страха, запугивание. Также в рамках кибератак для исполнителя гораздо проще скрыть свою личность, равно как и непосредственный источник нападения (при необходимости). В конечном итоге, учитывая тот факт, что в киберпространстве идентичность, границы между государствами легко размываются, данная проблема может в полной мере являться не проблемой одного, конкретного государства, а обладать

[87] Graham D. Cyber Threats and the Law of War // Journal of National Security Law & Policy. - 2010. - Vol. 4. P. 96.

характерными транснациональными чертами[88]. Также необходимо отметить экономический эффект при использовании данных инструментов – как отмечалось в рамках данной работы несколько ранее. Использование киберплатформы для атак приводит к максимально эффективному в соотношении вкладываемых ресурсов и выгод, с точки зрения той или иной организации, имеющей меньшие ресурсы и возможности, нежели государства, при том условии, что кибертерроризм может причинить значительный ущерб без прямых жертв, но выполнив свои функции – запугав население, нарушив обычный ход жизни в том или ином государстве[89]. Исходя из этого вполне логично в рамках данной работы сделать допущение о том, что киберпространство последовательно трансформируется в новую область противодействия, для которой будет характерна, и конкуренция за сферы влияния, и разработка новых способов воздействия на своего оппонента. Учитывая тот факт, что стратегическая мысль о войне в киберпространстве находится на своих начальных стадиях, тем не менее, многими крупными государствами разработаны своеобразные наступательные операции в киберпространстве, в том числе, функционируют подразделения, имеющие навыки для оборонительных кибероперациий – иными словами, начиная с XXI ст., киберпространство используется государствами в качестве платформы для обеспечения эффективности проведения военных операций, включая такие аспекты как шпионаж, дестабилизация оппонента и т.д[90].

Так, в 2005 году в американском киберпространстве специалистами были обнаружены китайские внедренные пользователи и программы, проникшие в многочисленные системы безопасности, включая Министерство обороны США, Государственный Департамент США, Министерство национальной

[88] Bendovschi A. Cyber-Attacks – Trends, Patterns and Security Countermeasures // Procedia Economics and Finance. 2015. [Electronic resource] URL: https://www.researchgate.net/publication/283967866_Cyber-Attacks_-_Trends_Patterns_and_Security_Countermeasures (accessed: 07.03.2019)

[89] Choucri N., Goldsmith D. Lost in cyberspace: harnessing the Internet, international relations, and global security // Bulletin of the Atomic Scientists. – 2012. – Vol. 68. P. 74.

[90] Duić I., Cvrtila V. International cyber security challenges // MIPRO. 2017. [Electronic resource] URL: https://bib.irb.hr/datoteka/878827.Duic_Cvrtila_Ivanjko_International_cyber_security_challenges_.pdf (accessed: 07.03.2019)

безопасности и т.д., что вынудило крупнейшие государства мира ускорить развитие потенциала для функционирования компьютерной инфраструктуры и безопасности[91].

Так, применимо к таким крупным странами как США и Китай стоит отметить, что оба государства в процессе строительства своей концепции связанной с действиями в киберпространстве руководствуются различными внешнеполитическими приоритетами в процессе развития своего кибернетического потенциала. Так, в случае с Китаем стоит отметить, что данное государство развивает свои возможности осуществления боевых действий в киберпространстве в качестве прямого ответа на характерные изменения в геополитической конкурентной среде. В данном контексте стоит отметить, что основные принципы данного взаимодействия изложены в Военно-стратегическом руководстве, которые являются стимулом для Китая в осуществлении борьбы за военное доминирование с помощью развития возможностей ведений войны в киберпространстве.

С другой стороны США развивают военный потенциал для решения проблем киберпространства в силу уязвимости своей национальной инфраструктуры, в том числе в области телекоммуникаций, энергетики, финансов, банковского дела, транспорта, аварийных служб. Документ, который подкрепляет данные усилия, является Директива 63, которая была разработана Советом национальной безопасности в 1998 году. Данный документ предназначен для решения «проблем растущих потенциальных возможностей атак против США в силу того факта, что безопасность экономики США зависит от противодействия различным нетрадиционным атакам на информационные системы, информационную инфраструктуру США»[92].

[91] Digital Europe: Pushing the frontier, capturing the benefits / McKinsey Global Institute. June 2016 [Electronic resource] URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20europe%20pushing%20the%20frontier%20capturing%20the%20benefits/digital-europe-full-report-june-2016.ashx (accessed: 01.03.2019)

[92] U.S. Presidential Decision Directive/ NSC-63. May 22, 1998 // [Electronic resource] URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm (accessed: 07.03.2019)

Таким образом, мы можем говорить о том, что во многом, развитие кибернетического потенциала для самообороны связано с неореалистической теорией, исходя из которой, государства не могут полагаться на своих союзников, негосударственных субъектов в процессе защиты своих ресурсов и интересов. Кроме этого, свидетельством кибератак является такой показатель как конкуренция за военное превосходство в киберпространства, а само обеспечение безопасности киберпространства является главным приоритетом национальной безопасности фактически любого государства.

ГЛАВА 2. ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ГЛОБАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ В МЕЖДУНАРОДНОМ ФОРМАТЕ

2.1. Вопросы обеспечения глобальной кибербезопасности

В условиях современных глобальных угроз, последовательное и всестороннее обеспечение безопасности в мире, требует от всех заинтересованных участников координации в процессе урегулирования различных возникающих политических и экономических вопросов, в том числе, в контексте формирования грамотного ответа на данные угрозы, включая область обеспечения безопасности. В своем практическом воплощении данный тезис проявляется в том, что подобные вызовы могут быть воплощены в появлении очагов гражданских конфликтов, конфликтов на межэтнической почве, войн, либо в виде определенные продовольственных угроз, негативных последствий связанных с изменением климата, Загрязнением окружающей среды, истощением природных ресурсов, войнами за данные ресурсы, замедлением повторного возобновления ресурсов, либо в виде необходимости развития зеленой экономики, рационального использования природных ресурсов и т.д[93]. Тем не менее, среди всего спектра компонентов обеспечения безопасности, относительно новым и достаточно сложным элементом безопасности является кибербезопасности. В данном контексте стоит отметить, что само понятие кибербезопасности включает в себя целый спектр проблем самого различного типа, включая сопоставимое с проблемами количество решений. Кроме этого важно понимать, что кибербезопасности достаточно сильным образом связана с интернет-безопасностью и включает в себя такие аспекты обеспечения безопасности как устранение технических проблем, уязвимостей, включая такие специфические аспекты как социальные, поведенческие проблемы, противодействие криминальной деятельности в киберпространстве и т.д., в результате чего сфера киберпространства является

[93] Джаббарова К.Ф. Современные аспекты кибербезопасности в мире в контексте глобальных угроз // АНИ: Экономика и управление. - 2017. - №. 2. С. 323.

сложной системой в контексте обеспечения совокупной безопасности общества на современном этапе.

С другой же стороны, по мнению исследователей, «кибербезопасность является разделом безопасности, изучающей процессы формирования, функционирования, эволюции киберобъектов с целью последовательного выявления источников киберопасности, которые могут нанести ущерб киберобъектам, в том числе, в рамках кибербезопасности формируются законы, нормативные акты, регламентирующие термины, правила, требования, методики и рекомендации, выполнение которых может гарантировать защищенность киберобъектов от всех изученных источников киберопасности»[94], тогда как непосредственно под киберобъектом в рамках данного подхода подразумевается фактически любой объект, функционирование которого осуществляется с прямым либо косвенным участием различных программных средств.

Также важно отметить, что в своем системном изучении нуждаются киберпреступления, в силу того, что данный фактор в современном мире имеет статус глобальной проблемы, которая проявляется с помощью мошенничества, получения неправомерного доступа к компьютерной информации, распространении вредоносных программ и т.д. В данном контексте, анализируя различные подходы к понимаю киберпреступления, такие исследователи как Е. Шевченко приходят к выводу, что «системообразующим фактором, объединяющим различные виды преступлений, является компьютерная информация в качестве важнейшего элемента взаимодействия и отражения механизмов подготовки, совершения, сокрытия преступных деяний этого рода, выступающая в роли предмета или средства преступления. Для расследования преступлений, которые совершаются в киберпространстве, требуются и технические, и теоретические познания»[95].

С другой же стороны, важно понимать, что в современных условиях глобализации закономерно с каждым годом растет ущерб, которые несут

[94] Алпеев А.С. Указ. Соч. С. 40.
[95] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: Автореф. дисс. ... канд. юрид. наук: 12.00.12. - М., 2016. С. 16.

крупные организации, компании и отдельные граждане от кибератак и нападений злоумышленников. Так, исходя из прогнозов компании Gartner, «ежемесячные расходы корпораций и компаний мира на повышение безопасности системы информационных технологий составляют приблизительно $114 млрд., а в 2019 году прогнозируется рост на 8,7 процентов до $124 млрд., тогда как в целом рост киберрисков за 2017 год обошелся мировой экономике более чем в $450 млрд.»[96]. Во многом, дополняя данный тезис стоит отметить, что риски, связанные непосредственно с кибершпионажем, иными преступлениями в сфере интернет-деятельности, с каждым годом несут все большие угрозы для современного бизнеса и государственных структур, что предполагает разработку со стороны крупнейших государств и корпораций мира новых методов и инструментов для обеспечения кибербезопасности в целом.

Также, в отношении киберпреступлений стоит отметить, что к наиболее заметным действиям относится похищение данных, нарушение неприкосновенности частной жизни, кража интеллектуальной собственности, вымогательства, диверсии, что становится возможным в силу изученности системы защитных механизмов, отсутствии детальных исследований и разработки новых актуальных инструментов противодействия, организованного обмена информацией и т.д. Тем не менее, многие государственные организации, равно как и субъекты рыночных отношений, коммерсанты, физические лица, уделяют относительно небольшое значение проблемам и серьезной организации мероприятий направленных на последовательное повышение надежности системы кибербезопасности и не проводят эффективных работ по увеличению эффективности работы элементов кибербезопасности, повышению эффективности и рациональности защитных механизмов киберпространства, устойчивости и надежности Интернет-сети.

В данном контексте примечательным видится мнение С. Кузнецова, по мнению которого «современные достижения в технологиях вызывают

[96] Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019 // [Electronic resource] URL: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 (accessed: 08.03.2019)

значительные расширения киберпространства что приводит к последовательному изменению способа взаимодействии, способов и методов ведения бизнеса, сотрудничества как отдельных людей, так и компаний, правительственных организаций в рамках данных направлений. Одновременно с этим, наличие серьезной зависимости общества от различных цифровых инфраструктур, включая Интернет, делает данную инфраструктуру стратегическим национальным достоянием, достоянием, которое необходимо защищать для обеспечения благополучия и безопасности каждого отдельного народа и нации»[97].

В данных условиях важно понимать, что с целью формирования грамотных инструментов обеспечения глобальной кибербезопасности необходимо внимательное рассмотрение, выявление основных факторов и причин, которые побуждают злоумышленников к своим противоправным действиям, с целью разработки новых, эффективных, практичных механизмов в борьбе против хакеров, злоумышленников, вредителей среды киберпространства и инфраструктуры. Кроме этого, в условиях глобализации и быстрого расширения географии хакерских атак, преступных деяний киберпреступников и злоумышленников, важным аспектом видится координация, мобилизация умственных, интеллектуальных, научных, человеческих ресурсов против борьбы с киберпреступлениями по всему миру – во многом, данные компоненты и механизмы должны соответствовать текущим потребностям общества в контексте защиты данного общества от любых неправомерных проявлений со стороны отдельных лиц и заинтересованных в этом сторон, осуществляющих свои действия в киберпространстве.

Кроме того, на данный момент актуальным направлением видится совершенствование механизмов, правил многостороннего международного документа, играющего существенную роль в координации усилий всего мирового сообщества по вопросам кибербезопасности, в частности, упомянутой

[97] Кузнецов С. Кибербезопасность в 21 веке // [Электронный ресурс] URL: https://www.osp.ru/os/2013/05/13036002/ (дата обращения: 09.03.2019)

ранее Европейской Конвенции по киберпреступлениям 2001 г., которая содержит классификацию компьютерных преступлений, характерные рекомендации ля органов законодательной и исполнительной власти государств в плоскости борьбы с киберпреступлениями.

В данном случае также важно отметить, что характерные элементы и составные части кибербезопасности, в силу развития современного общества, постоянно совершенствуются, в том числе, расширяется и сфера влияния данных инструментов, исходя из чего важными видится глубокое изучение составляющих элементов, сущности теоретических аспектов кибербезопасности в мире и противодействия появлению новых угроз в киберпространстве[98].

Исходя из этого, в рамках данной работы представляется целесообразным определение основных угроз, свойственных для современного киберпространства и вызовов для кибербезопасности в целом:

1.Защита каналов передачи данных – обеспечение безопасности ресурсов Интернет (пакеты передачи данных, безопасность сетей, данных пользователей);

2.Защита телекоммуникационной инфраструктуры – совершенствование существующей инфраструктуры телекоммуникационных сетей – гаджетов, спутниковой связи, широковещательных сетей, микроволновых устройств:

3.Защита Интернет-сети – защита глобального пространства Интернет-сети, согласование глобальной оверлейной сети, характерных составных компонентов;

4.Защита компьютерных устройств – обеспечение безопасности серверов, станций пользователя от взломов хакеров, иных злоумышленников, совершенствование антивирусов, иных средств суть которых сводится к борьбе с вредоносными элементами;

5.Защита приложений – повышение эффективности и надежности приложений, связанных с передачей данных, иной информацией, включая совершенствование защиты от противоправных действий субъектов киберпространства:

[98] Von Solms R. From information security to cyber security // Computers & security. – 2013. – Vol. 38. P. 99.

6.Защита данных – обеспечение комплексной защиты данных участников киберпространства (юридическая защита, техническая защита, социальная защита, конфиденциальность);

7.Защита основных услуг – обеспечение безопасности оказания основных услуг в киберпространстве. Повышение эффективности сетей в контексте передачи данных, обеспечение стабильной работы ключевых для данной инфраструктуры служб;

8.Защита личности граждан – обеспечение подлинности пользователей киберпространства, формирование и организация работы основанной на принципах доверия, безопасного управления личными данными, включая формирование и развитие надежной системы защиты личных данных, включая юридические аспекты и конфиденциальность;

9.Защита государственных интересов – в данном случае, данный аспект проявляется через разработку и осуществление инструментов, механизмов, схем действия в киберпространстве направленном на защиту государственных интересов в рамках киберпространства;

10.Защита национальных интересов – последовательное и всестороннее обеспечение национальных интересов в киберпространстве с предусмотренными механизмами оперативного реагирования на возникающие вызовы и угрозы;

11.Защита региональных интересов – координация региональных аспектов и проблем связанной с кибербезопасности на региональном уровне;

12. Защита международных интересов – активное участие государства в деятельности направленной на повышение эффективности существующих систем кибербезопасности в мире, разработка, формирование, тестирование и интеграция новых инструментов, направленных на совокупное повышение эффективности противодействия кибератакам и повышения стабильности систем кибербезопасности в мире.

В конечно итоге, как видно из данного списка, с целью последовательного обеспечения общей и совокупной кибербезопасности в мире, в том числе, с целью последовательного укрепления киберзащиты, наибольшие усилия

требуются в плоскости обеспечения защиты каналов передачи данных, безопасности ресурсов, прочности телекоммуникационной инфраструктуры, защите государственных, региональных, международных интересов.

Тем не менее, проблемы кибербезопасности и сущность кибербезопасности в целом не может трактоваться всеми исследователями однозначно. Так, к примеру, Б. Геральд отмечает, что «для кибербезопасности более характерны не только проблемы, непосредственно связанные с киберпространством, сколько одновременно с этим существующие проблемы в технической, правовой, государственной, культурной, экономической плоскости»[99]. Иными словами, по мнению исследователя, в своем фактическом воплощении кибербезопасность выступает в качестве элемента противодействия таким проявлениям как терроризм, вредительство, дестабилизация в плоскости киберпространства. Кроме этого, учитывая масштабы возможного вреда в мировом масштабе, элемент кибербезопасности в киберпространстве закономерно занимает одно из ведущих мест в плане приоритетного направления для государств по всему миру, от которых требуется разработка, применение действенных, практических мер во многих областях информационной среды, системы кибербезопасности и повышения устойчивости данной системы.

В указанном контексте необходимо отметить, что специалисты Австрийского центра по кибербезопасности отмечают, что «важно учитывать все проблемы и вопросы напряженности в отношениях между неприкосновенностью личной жизни и государственной безопасностью, Защитой людей, государства от кибератак, угроз кибервойн, кибертерроризма, что предполагает мониторинг и отслеживание фактов кибершпионажа с целью пресечения данных проявлений и обеспечения действенных практических мер пресечения данных действий в

[99] Gerald B.F. The theory the intersectionality can make cyber security collaboration real // [Electronic resource] URL: https://techcrunch.com/2015/02/17/the-theory-of-intersectionality-can-make-cybersecurity-collaboration-real/ (accessed: 08.03.2019)

киберпространстве, включая соблюдение этики, норм международного права»[100].

Во многом, следует допустить, что проблемы кибербезопасности являются проблемами глобального (мирового) масштаба и относительно новым направлением для работы современных исследователей, исходя из чего неизученные элементы, связанные с кибербезопасностью нуждаются в более детальном анализе с целью совершенствования инструментов противодействия деятельности злоумышленников. В данном контексте стоит отметить, что А. Кохен пришел к выводу, что «необходимо перенести центр внимания на преступления хакеров и кибератак, которые больше всего связаны с массивными информационными или электронными ресурсами компаний и правительств стран мира. Пришло время заострить наше внимание на приоритетных задачах, обеспечить безопасность информационных массивов и в целом разработать новые стратегии для безопасности киберпространства»[101]. Иными словами, многие исследователи справедливо приходят к допущениям, что новые и сложные международные угрозы (в лиц хакеров, злоумышленников в киберпространстве) нуждаются в формировании сильной и системной конструкции направленной на защиту киберпространства с целью обеспечения полноценной, эффективной безопасности данного пространства в долгосрочной перспективе. Во многом, для решения данной задачи для оказания активного противодействия, требуется последовательное повышение безопасности цифровой инфраструктуры в каждом отдельном государстве, развитие наступательного, оборонительного потенциала системы информационно-телекоммуникационной инфраструктуры, с целью грамотного противодействия кибератакам.

Кроме этого, по мнению Н. Ройтера, «кибератаки являются средством борьбы против государства, средством которое может застать своих

[100] Henry A. Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry // [Electronic resource] URL: https://unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdfRequirements (accessed: 10.03.2019)

[101] Cohen A. The Willie Sutton Theory of Cyber Security // [Electronic resource] URL: https://www.illumio.com/blog/willie-sutton-cyber-security#gsc.tab=0 (accessed: 10.03.2019)

противников в самый неподходящий момент учитывая тот факт, что кибератаки не сопровождаются, по сути, чрезмерными затратами человеческого и финансового ресурса, однако также эффективно могут разрушать определенные коммуникации и экономику отдельного государства»[102]. По своей сути, характер происходящих в мире кибератак характеризуется для каждого объекта атаки своей неожиданность, разрушением и нанесением убытков. Также в определенных случаях данные атаки могут быть направлены не на государство, а на завладение определенной информацией бизнес-процессов, либо передачи данной информации, с целью похищения финансовых средств, распространения компромата в необходимое время и т.д.

С другой стороны, Х. Салим, изучая проблемы теоретического аспекта кибербезопасности и совокупной минимизации рисков бизнес-процессов пришел к заключению, что «нынешние подходы в организации кибербезопасности имеют ограниченную эффективность – ежегодно крадутся основные данные бизнес-процессов и в данных случаях отмечена высокая роль хакеров, которые взломали рабочую станцию, иные средства киберпространства, на что специалисты не могут объективно и уместно отреагировать»[103].

Иными словами, киберпространство нуждается в последовательной минимизации последствий от системных угроз, умышленных воздействий, исходя из чего важным направлением противодействия видится разработка и осуществления более совершенной концепции компьютерной безопасности в сфере киберпространства, осознания актуальности в широком смысле проблемы кибербезопасности и развития стратегий безопасности киберпространства в целом.

В своей совокупности проблема последовательного изучения характера и сущности элементов, концептуальных основ кибербезопасности, эффективности данных основ предполагают формирование единого подхода к разработке

[102] Rueter N. The Cybersecurity Dilemma.Department of political science Duke University // [Electronic resource] URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.826.7847&rep=rep1&type=pdf (accessed: 10.03.2019)
[103] Salim H. Cyber safety: A systems thinking and systems theory approach to managing cyber security risks. - Massachusetts Institute of Technology, 2014. P. 42.

действенных систем и механизмов кибербезопасности, разработки и осуществления рациональных мер направленных на функционирование киберпространства, обеспечение защиты данного пространства от киберпреступлений, включая процесс разработки надежных механизмов и сервисов для противодействия кибератакам и обеспечения применения новых интеллектуальных методов направленных на совершенствование системы кибербезопасности, предотвращение попадания вирусных элементов и своевременного выявления, нейтрализации возможных атак[104].

Так, по мнению М. Безкоровайного и А. Татузова, «кибербезопасность охватывает как информацию в качестве объекта защиты, так и технические средства, которые определяют возможность функционирования информации, защиту способов функционирования новой сущности – киберпространства. Фактически, защищается не только информация, а сама деятельность людей, которая осуществляется с помощью информации, распространяемой с помощью технической инфраструктуры, информационно-коммуникационных технологий»[105].

Фактически, кибербезопасность обеспечивает защищенность киберпространства с помощью сохранения конфиденциальности, целостности, доступности информации в данном пространстве, в рамках чего существует сетевая безопасность, бесперебойные, безопасные способы передачи данных и т.д. Фактически, при эффективности системы кибербезопасности также минимизируется возможность злоумышленников проникнуть в защищаемые участки киберпространства, тогда как формирование элементов киберпреступлений в киберпространстве обуславливает четкие механизмы средства по их нейтрализации и ликвидации с целью уменьшения убытков и ущерба.

[104] Hansen L., Nissenbaum H. Digital Disaster, Cyber Security and the Copenhagen School. University of Copenhagen, New York University // International Studies Quarterly. - 2009. - № 53. P. 1159.
[105] Безкоровайный М.М., Татузов А.Л. Кибербезопасность - подходы к определению понятия // Журнал Вопросы кибербезопасности. – 2014. - №1. С. 24.

Таким образом, обобщение, раскрытие причин киберпреступлений является важной задачей для формирования новых инструментов в сфере обеспечения кибербезопасности. В данном контексте важным направлением видится точное составление классификации и элементов опасности в киберпространстве, изучение данных элементов, характеристика их сущности с определением основных особенностей, их тактики, действий злоумышленников с целью формирования новых механизмов и инструментов для пресечения данных деяний в киберпространстве.

На сегодняшний день, характерные вопросы обеспечения кибербезопасности, как уже отмечалось в рамках данной работы несколько ранее, затрагивают все мировое сообщество. Во многом, глобальное информационное пространство, будучи достаточно большой совокупностью различных информационных ресурсов и составных инфраструктур, которые могут являться и государственными, и межгосударственными информационными сетями, телекоммуникационными сетями общего пользования и трансграничными каналами передачи данных, являются важнейшими сопутствующими частями деятельности фактически любого государства. На момент 2018 г., число использующих глобальную сеть, составляет около 3.6 млрд. человек, и в данном случае Российская Федерация, на момент 2015 года занимала шестое место по количеству интернет-пользователей[106]. С другой же стороны, являясь одним из главных достижений современности, глобальная сеть также является благоприятной почвой для совершения различных преступлений. Тем не менее, на сегодняшний день достаточно сложно обобщить существующие компьютерные преступления по причине их многогранности и сложности, что также усложняет и отражение механизмов противодействия данным угрозам.

В данном контексте важно понимать, что совокупное понятие «кибербезопасности» последовательно содержит в себе великое множество

[106] Бураева Л.А. О Некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. - 2015. - № 13. С. 96.

составных (производных) проблем различного типа, среди которых важное место отводится защите данных, компьютерных систем, каналам передачи данных, телекоммуникационной инфраструктуры и других аспектов, отмеченных в рамках данной работы несколько ранее.

Тем не менее стоит отметить, что, к примеру, в российских нормативный актах и научной литературе, достаточно часто используется именно понятие «информационная безопасность», которое характеризует все аспекты, связанные с определением, достижением, формированием, поддержанием конфиденциальности, целостности, доступности, подотчетности и достоверности информации, и средств обработки информации[107]. В данном контексте стоит отметить, что по мнению аналитиков, основная цель атак злоумышленников заключается не только в завладении информационными данными но и во влиянии на программные средства, которые формируют информационную инфраструктуру, цифровые системы управления исходя из чего термин «кибербезопасность», и другие производные понятия («киберугроза», «киберпространство», «кибероружие», «кибератаки» и т.д.), требуют осмысления, формализации, что на сегодняшний день является областью активных исследований и разработок, с использованием комплексного и всестороннего подхода.

Так, в 2014 году Советом Федерации для обсуждения был предложен проект Концепции стратегии кибербезопасности РФ, в которой были определены основные направления усилий государства, прикладываемых в отношении противодействия новым угрозам, которые возникают в современном информационном мире. Так, в проекте указанной Концепции авторами было отмечено, что «в настоящее время в Российской Федерации существует ряд документов, направленных на обеспечение различных аспектов национальной информационной безопасности, однако они не охватывают в необходимой мере систему отношений, возникающих в рамках киберпространства как элемента

[107] Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы: дис. ... докт. наук: 23.00.04. - М., 2017. С. 24.

информационного пространства»[108]. Как результат, в проекте Концепции разработчиками были даны определения таких понятий как «информационное пространство», «киберпространство», «кибербезопасность», которая определена как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями»[109]. К данному аспекту необходимо добавить и тот факт, что на сегодняшний день в научной и исследовательской плоскости продолжается активное обсуждение, данное Концепции и встречается мнение исследователей, делающих акцент на возможных направлениях совершенствования данной Концепции (уточнение понятий, определение иных терминов и т.д.).

Кроме этого, на сегодняшний день, среди основных тенденций развития киберугроз в рамках данной работы следует назвать стремительное увеличение числа кибератак, повышение сложности, многогранности атак, которые включают в сея несколько этапов атаки, включая специальные методы защиты от их нейтрализации, воздействие и направленность данных атак на цифровые устройства, мобильные устройства, которые подвержены несанкционированному доступу, что сопровождается ростом числа атак на информационную инфраструктуру крупных корпораций, промышленных объектов, государственных структур, включая используя отдельным государствами средств и методов кибернападанеия на другие государства – во многом, данные угрозы также подтверждаются многочисленными фактами применения данных инструментов и ростом числа киберпреступлений в мире в целом.

Кроме этого, по данным проведенного Университетом Мэриленда исследования, каждые 39 секунд жертвами киберпреступников становится каждый третий[110], и как правило, наиболее успешные атаки направлены на

[108] Концепция стратегии кибербезопасности Российской Федерации (проект) // [Электронный ресурс] URL: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 09.03.2019).
[109] Там же.
[110] Hackers Attack Every 39 Seconds / Security. February 10, 2017 [Electronic resource] URL: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds (accessed: 09.03.2019)

серверы и компьютеры конечных пользователей, подключенных к глобальной сети с помощью бот-сетей, фишинга, распределенных атак «человек посередине», «отказ в облуживании» и т.д[111].

На сегодняшний день, к устройствам наиболее высокой степени уязвимости в плане информационной безопасности относятся мобильные устройства. Так. Используемая платформа «Android», доля которой на рынке доходит до 80%, основана на открытом коде, который может быть подконтролен различным службам в странах Запада (главным образом, в США), что создает реальную угрозу для национальной безопасности любой страны, переводя данную страну под возможное влияние иностранных спецслужб[112]. Примечательно, что при этом доля разрабатываемых программ, для данной системы, по мнению исследователей, стремительно возрастает и составляет более 90% от общего количества вирусов.

Как результат, обеспечение кибербезопасности в данном случае заключается в развитии производства электронных изделии, каналов сбыта инфокоммуникационных решений внутри страны. С целью комплексного решения проблем, связанных с кибербезопасностью важно организовывать ряд системных НИОКР, среди компетентных организаций и предприятий для обеспечения вывода на рынок новых продуктов мирового уровня, что позволит государству на федерльном уровне сформировать защищенную инфраструктуру кибербезопасности. Обеспечить развитие экономики на основе производства отечественных инфокоммуникационных решений. Кроме этого, деятельность государства может быть направлена на создание механизмов, связанных с так называемой «автономностью интернета», что в 2019 году активно продвигается в отечественных политических кругах и связана с обеспечение кибербезопасности, защитой значимых государственных и промешенных объектов нападения на которых могут существенным образом повлиять на

[111] 13 Alarming Cyber Security Facts and Stats // [Electronic resource] URL: https://www.cybintsolutions.com/cyber-security-facts-stats/ (accessed: 09.03.2019)
[112] Згоба А.И., Маркелов Д.В. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. - 2014. - № 5. С. 30.

обеспечение безопасности Российской Федерации, учитывая что различные программы могут остановить работу как отдельных предприятий, заводов так и отдельных атомных электростанций.

Также ежегодно фиксируются многочисленные атаки на различные банки мира – в октябре 2014 года, экспертами была выявлена вредоносная сеть из 500 000 компьютеров, которая использовала контрольную панель на удаленном сервере для сбора данных, в результате чего похитители собрали около миллиона пар логин-пароль, которые были связаны с системами онлайн-банкинга в европейских и американских банках.

Кроме этого, в феврале 2015 года стало известно о хакерской операции «Carbanak», в процессе которой злоумышленники сумели украсть более $1 млрд., из 10 финансовых организации из 30 стран мира[113].

Также все большие обороты набирают преступления в киберпространстве связанные с террористической, экстремисткой направленностью – к примеру, еще на момент 1998 года около 30 террористических организаций имели свои сайты, а на сегодняшний день число подобных ресурсов более 1000[114].

Также с каждым годом информационное пространство все более активно используется для хищения государственных секретов – к примеру, в 2013 году «Лабораторией Касперского» была раскрыта сеть «Красный Октябрь», которая с 2008 по 2013 гг., занималась хищением государственных секретов и представляла собой комплекс вредоносных программ, которыми были заражены компьютеры различных правительственных структур, посольств, научных институтов и организаций, которые действовали в РФ, странах СНГ, Западной Европе, Австралии и США[115].

Так можно говорить о том, что проблемы, существующие в сфере кибербезопасности на современном этапе не могут быть в полной мере решены

[113] Osborne Ch. Carbanak hacking group steal $1 billion from banks worldwide // [Electronic resource] URL: https://www.zdnet.com/article/carbanak-hacking-group-steal-1-billion-from-banks-worldwide/ (accessed: 10.03.2019)
[114] Бураева Л.А. Информационные войны и информационный терроризм в современном мире: методы и поле действия // Известия Кабардино-Балкарского научного центра РАН. - 2014. - № 1. С.9.
[115] «Лаборатория Касперского» раскрыла шпионскую сеть «Red October» // [Электронный ресурс]. URL: http://24gadget.ru/1161053174-laboratoriya-kasperskogo-raskryla-shpionskuyu-set-red-october.html (дата обращения: 11.03.2019).

традиционными средствами, требуют системного подхода в создании комплексных систем кибербезопасности, систем которые могут противостоять новым и актуальным вызовам и угрозам, что может быть достигнуто с помощью координации международных усилий, государственных органов в различных странах и общества в целом с целью полноценного решения вопросов кибербезопасности с использованием различных версий телекоммуникационного оборудования, программного обеспечения, средств защиты информации.

2.2. Усилия международных акторов и организаций в процессе обеспечения кибербезопасности

Еще 10 мая 1999 Генсек ООН Кофи Аннан выступил с докладом (A / 54/213), в котором признавалось наличие проблемы в сфере международной информационной безопасности. Резолюция 53/70 положила начало обсуждения необходимости создания нового международно-правового режима для регулирования сферы информационного пространства, ИКТ и методов ее использования[116]. В 1999 г. в Женеве проходил международный семинар по вопросам МИБ в котором принимали участие представители более 50-ти стран. На 54 сессии Генеральной Ассамблеи ООН был предложен проект резолюции «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», в котором впервые высказывалась озабоченность возможности потенциального использования средств ИКТ «с целями, что несовместимы с задачами обеспечения международной стабильности и безопасности», что может негативно повлиять на безопасность государств, как в гражданской, так и в военной областях. Считая необходимым предотвращение «неправомерного использования информационных ресурсов,

[116] Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г.: Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // [Электронный ресурс]. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 02.03.2019)

либо технологий в террористических и преступных целях», ГА ООН поставила вопрос о «целесообразности разработки международных принципов, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствование борьбы с информационным терроризмом и криминалом»[117]. Тем самым обеспечение информационной безопасности было признано глобальной проблемой современности в соответствии с Резолюцией 54/49 ООН от 1 декабря 1999 г[118]. Представители разных стран отмечали, что использование новых информационных технологий и средств воздействия высокоразвитых стран на менее технологичные страны мира привело к изменению глобального и регионального балансов силы, обусловило новые сферы конфронтации между традиционными и новыми центрами глобального противостояния, позволило достигнуть преимуществ в информационных технологиях и средствах манипулирования общественным сознанием для широкомасштабной экспансии с применением не ограниченных международным правом видов вооружений.

Проблема компьютерной преступности подробно рассматривалась во время проведения X Конгресса ООН в апреле 2000 г. Группой экспертов было предложено определение термина «киберпреступность», под которым понималось любое преступление, может быть осуществлен с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против них, то есть, по мнению экспертов, такие действия охватывают любое преступление в сфере ИКТ[119].

Также в апреле 2000 года состоялся X Конгресс ООН, во время которого была принята Венская декларация о преступности и правосудии: ответы на

---

[117] Информационные вызовы национальной и международной безопасности / под ред. А.В. Федорова. - М.: ПИР-Центр, 2001. С. 144.

[118] Резолюция Генеральной Ассамблеи ООН 55/63 от 22 января 2001 г.: Борьба с преступным использованием информационных технологий // [Электронный ресурс]. URL: http://www.ifap.ru/ofdocs/un/5563.pdf (дата обращения: 04.03.2019)

[119] Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями (Вена, 10–17 апреля 2000 г.) Преступления, связанные с использованием компьютерной сети: справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети // [Электронный ресурс] URL: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_R.pdf (дата обращения: 04.03.2019)

вызовы XXI века. В декларации было подтверждено решение разработать программные рекомендации по предупреждению преступлений, связанных с использованием компьютеров, а также усиливать сотрудничество по расследованию и судебному преследованию за преступления с использованием компьютеров и высоких технологий[120].

Кроме того, Экономическим и Социальным Советом ООН в 2000 году была принята Декларация министров «Развитие и международное сотрудничество в XXI веке: роль информационных технологий в контексте глобальной экономики, основанной на знаниях». Основную часть этого документа посвятили роли ИКТ в формировании глобальной экономики знаний, устойчивого развития наций, искоренению бедности, уменьшению цифрового разрыва между странами и обеспечения равного доступа каждого человека к ИКТ. Также, в документе подчеркивалось, что Экономический и Социальный Совет ООН может играть ключевую роль в обеспечении вышеупомянутых усилий, а также по вопросам информационной безопасности и киберпреступности[121].

В 2004 г. Российской Федерацией был подготовлен собственный документ – проект «Принципов, касающихся международной информационной безопасности», который был отмечен в докладе ГА ООН А/55/140 в качестве российского вклада в дальнейшие перспективы обсуждения данной проблемы. Документ содержит в себе основную понятийную базу и приводит ключевые определения МИБ, угроз информационной безопасности, понятие информационного оружия, информационных войн, терроризма и информационной преступности.[122]. Пять ключевых принципов МИБ из данного

[120] Венская декларация о преступности и правосудии: ответы на вызовы XXI века. Принята на Десятом Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, Вена, 10 – 17 апреля 2000 года // [Электронный ресурс] URL: http://www.un.org/ru/documents/decl_conv/declarations/vendec.shtml (дата обращения: 04.03.2019)

[121] Развитие и международное сотрудничество в XXI веке: роль информационной технологии в контексте основанной на знаниях глобальной экономики : Декларация министров на этапе заседания ЭКОСОС высокого уровня, принятая Экономическим и Социальным Советом от 7 июля 2000 года // [Электронный ресурс] URL: http://www.un.org/ru/development/ict/ecosoc_decl2000.htm (дата обращения: 04.03.2019)

[122] Международное сотрудничество в области информационной безопасности // [Электронный ресурс]. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/486848 (дата обращения: 04.03.2019)

документа отводятся под определение роли и права, обязательств и ответственности государств в информационном пространстве. Резолюцией от 29 ноября 2001 г. была одобрена идея создания к 2004 г. особой экспертной группы – Группы правительственных экспертов государств-членов ООН (ГПЭ) в целях систематического проведения всесторонних исследований проблематики МИБ[123]. Мандат данной Группы предусматривает рассмотрение потенциальных и существующих угроз в области информационной безопасности, а также возможных направлений по их совместному устранению.

В дальнейший период осуществляется реализация решения международного сообщества о необходимости широкого практического изучения вопросов МИБ, принимаются резолюции, развивают положения предыдущих резолюций. Так, 23 января 2002 г. ГА ООН принимает резолюцию по докладу на тему «Борьба с преступным использованием информационной технологии», где говорилось о необходимости международного сотрудничества, а также между государствами и частными сектором в борьбе с преступным использованием ИКТ, а также о необходимости содействия предоставления ИКТ развивающимся странам, поскольку несоответствия различных государств в уровне доступа к ИКТ и их использовании могут снизить эффективность борьбы с преступностью в этой сфере[124]. В 2002 г. на Общеевропейской конференции в Бухаресте была принята декларация, закрепившая принцип укрепления доверия и безопасности в процессе использования ИКТ. Она предусматривает разработку «глобальной культуры кибербезопасности», которая должна была обеспечиваться путем принятия превентивных мер и поддерживаться всей сообществом при условии сохранения свободы передачи информации. Страны согласились с тем, что необходимо осуществлять «предупреждение использования информационных технологий и ресурсов в преступных или

[123] Резолюция Генеральной Ассамблеи ООН 56/19 от 7 января 2002 г.: Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // [Электронный ресурс]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement (дата обращения: 07.03.2019)

[124] Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН 56/121 от 23 января 2002 [Электронный ресурс]. URL: //www.un.org/russian/documen/gadocs/56sess/56reslis.htm (дата обращения: 07.03.2019)

террористических целях», а также укреплять международное взаимодействие в данной сфере[125]. Документ предусматривает «приоритетные области действий» в сфере ИКТ. Среди них важное место отводится вопросам обеспечения безопасности информационных средств и технологий. Базируясь на принципе справедливого, адекватного и равного доступа к ИКТ государств, особое внимание сторонами уделялось угрозам потенциально военного использования ИКТ. Впервые в истории было отмечено, что эффективное обеспечение информационной безопасности может достигаться не только технологическими путями, но для этого также необходимы и соответствующие усилия в области правового урегулирования данного вопроса, а также выработка соответствующей национальной политики для каждой страны[126].

В соответствии с решениями резолюций ГА ООН 2001-2002 гг., в декабре 2003 г. в Женеве прошел первый этап Всемирной встречи по вопросам информационного общества на высшем уровне. Данная встреча ознаменовала собой первый в истории международный форум, где происходило обсуждение вопросов, непосредственно связанных с глобальными информационными процессами по информатизации. В конференции принимал участие более 11 тыс. представителей 176 государств мира, включая и представителей международных организаций. В процессе встречи вопросов по МИБ находились в центре повестки дня. Так, итогом первого этапа данного события стало принятие сразу двух важных документов: Декларации принципов и Плана действий. Эти два документа охватывают в себе различные аспекты формирования глобального информационного пространства и общества, а также главные направления в области межгосударственного взаимодействия по данной проблеме, учитывая создание и развитие информационно-коммуникационной инфраструктуры, безопасности использования ИКТ, безопасного доступа к информации,

[125] Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН 56/121 от 23 января 2002 [Электронный ресурс]. URL: //www.un.org/russian/documen/gadocs/56sess/56reslis.htm (дата обращения: 07.03.2019)

[126] Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии 12 декабря 2003 г. // [Электронный ресурс]. URL: http://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения: 07.03.2019)

инфраструктуре, а также услуг, базирующихся на ИКТ. Декларация принципов указывает на то, что укрепление основ для доверия, с учетом информационной безопасности и безопасности сетей, можно рассматривать в качестве предпосылки для становления полноценного информационного общества[127].

Важные аспекты борьбы с информационной преступностью были зафиксированы в резолюции ГА ООН от 30.01.2004 года «Создание глобальной культуры кибербезопасности и защита важнейших информационных структур»[128]. Существенными из них можно назвать формулировку перечня элементов для защиты важнейших информационных инфраструктур. То есть были указаны те защитные механизмы, как международного, так и национального уровней, которые являются базовыми элементами для построения глобальной системы противодействия попыткам использования и использованию ИКТ в целях несовместимых с основными принципами международного права и безопасности государств, общества и личности.

В рамках ООН звучат призывы к разработке единого универсального документа по МИБ, который бы учел новые вызовы международному миру и безопасности, а также интересы международного сообщества. Такие мысли были озвучены во время проведения XII Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, который проходил в Бразилии в апреле 2010 года. И хотя такая позиция не была поддержана единогласно, обсуждение этой темы на уровне ООН является значительным шагом вперед. Также, государства выразили обеспокоенность, что развитие ИКТ и увеличение площади использования сети Интернет способствуют росту преступности, создают новые возможности для преступников[129].

---

[127] Всемирная встреча на высшем уровне по вопросам информационного общества // [Электронный ресурс]. URL: http://www.un.org/ru/events/pastevents/wsis.shtml (дата обращения: 08.03.2019)

[128] Резолюция Генеральной Ассамблеи ООН от 23 декабря 2003 г.: Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур // [Электронный ресурс]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/54/PDF/N0350654.pdf?OpenElement (дата обращения: 08.03.2019)

[129] Резолюция ГА ООН A/RES/65/230 «Сальвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в

Во время проведения XII Конгресса ООН среди других вопросов в повестку дня был включен вопрос последних тенденций в использовании научно-технических достижений правонарушителями и компетентными органами борьбы с киберпреступностью. Основными проблемами, связанными с киберпреступностью, были определены следующие: 1) непонятность масштабов киберпреступности, поскольку статистика не отражает истинное положение вещей; 2) транснациональный характер киберпреступности, поскольку преступления в киберпространстве не ограничены физическими границами, а соответствующие органы реагирования обязаны проводить расследования с соблюдением обязательного принципа государственного суверенитета, а поэтому им необходимо получить соответствующее разрешение, что в свою очередь требует много времени, а скрыть следы преступления можно за минуты; 3) различные национальные законодательные подходы, когда киберпреступление может быть совершено на территории государства, законодательство которой не предусматривает наказания за такой вид преступления. Согласно этим проблемам ООН выступает за начало международного сотрудничества по стандартизации законодательства, разработке модельного законодательства, типичных законов и технической стандартизации в пределах определенного региона[130]. Таким образом, подавляющее большинство участников XII Конгресса ООН поддержали начало переговоров о создании нового международного документа по вопросам МИБ, который мог бы быть принят в форме дополнительного протокола к Конвенции ООН против транснациональной организованной преступности или отдельного документа, который бы усовершенствовал и дополнил положения существующих региональных договоров. Однако не все поддержали эту

изменяющемся мире» // [Электронный ресурс] URL: : http://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration.shtml (дата обращения: 08.03.2019)

[130] Доклад о работе двенадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию (12–19 апреля 2010 г.) // [Электронный ресурс] URL: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053830r.pdf (дата обращения: 08.03.2019)

инициативу, а представители некоторых государств настаивали на том, что Конвенции Совета Европы достаточно для регулирования этого вопроса.

Результатом проведения XIII Конгресса ООН 12-19 апреля 2015 г. стало принятие «Дохинской декларации», в которой определено, что необходимо направить все усилия на создание защищенного и открытого киберпространства, предупреждать и противодействовать преступной деятельности с помощью сети Интернет, усиливать сотрудничество между правоохранительными органами, повышать уровень защищенности инфраструктуры государств, содействовать предоставлению технической помощи и повышению потенциала развивающихся стран, противостоять киберпреступности особенно в отношении кражи личных данных, вербовки с целью торговли людьми и защиты детей от сексуальной эксплуатации с помощью сети Интернет[131].

Стоит отметить и тот факт, что на 66-й сессии ГА ОНН в 2011 г. странами ШОС была выдвинута инициатива и проект «Правил поведения в сфере обеспечения МИБ», который был переиздан в новой редакции в 2015 г. и внесен на новое рассмотрение ГА ООН. Новая версия документа опирается, прежде всего, на миротворческий характер. Документ нацелен на предотвращение конфликтогенности в информационном пространстве мира, закрепляет обязательство государств не применения ИКТ, ведущих к нарушению международного мира и баланса сил, вмешательству во внутренние дела других держав, что может приводить к подрыву их государственной, политической и экономической стабильности. Также документ предусматривает обязательства государств к воздержанию от угроз и применения силы в разрешении международных конфликтов в информационной сфере[132].

---

[131] Дохинская декларация о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку дня Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности от 19 апреля 2015 г. // [Электронный ресурс] URL: https://www.unodc.org/documents/congress/Declaration/V1504153_Russian.pdf (дата обращения: 11.03.2019)

[132] Инициатива стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» // [Электронный ресурс]. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/916241 (дата обращения: 12.03.2019)

Также в рамках двустороннего взаимодействия по обеспечению международной информационной безопасности (МИБ) и, в частности, кибербезопасности можно привести пример РФ и Китая: в мае 2015 г. между правительствами РФ и КНР было подписано Соглашение «О сотрудничестве в сфере обеспечения международной информационной безопасности»[133]. Соглашением предусматривается создание организационно-правовых основ сотрудничества стран в сфере обеспечения международной информационной безопасности. Россия и Китая будут совместно реагировать на любые проявления и угрозы МИБ, к которым относятся, в частности: использование ИКТ для осуществления актов агрессии, направленных на нарушение суверенитета, безопасности, территориальной целостности государств; в целях причинения экономических и иных убытков, в том числе путем деструктивного влияния на объекты информационной инфраструктуры, с террористической целью, для пропаганды терроризма и привлечения к террористической деятельности новых сторонников и пр.

Вопреки реальным и гипотетическим экономическим и географическим ограничением указанные и подобные им организации все активнее берут на себя роль не только региональных, но и международных, распространяя сферы своих интересов безопасности и влияния на все мировое общество. Вместе с тем парадоксальным является тот факт, что у ряда региональных оборонительных структур и структур по обеспечению безопасности, в частности НАТО, Совета Европы, ОБСЕ, пока отсутствуют соответствующие амбиции международного уровня, и они до сих пор являются региональными структурами в контексте кибербезопасности. Даже упомянутая ранее Конвенция о киберпреступности Совета ЕС, которая фактически вышла за пределы не только географической, но и политической Европы, а между ее подписантов есть страны, географически весьма отдаленных от Европы (например, Япония), не может, по сути, считаться

[133] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики
о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. // [Электронный ресурс]. URL: http://www.mid.ru/foreign_policy/international_contracts/2_contract/-/storage-viewer/bilateral/page-38/43921 (дата обращения: 12.03.2019)

документом международного значения. Сейчас это существенно усложняет присоединение к этому документу ключевых стран. Активна нормотворческая и институционально-организационная деятельность по кибербезопасности на национальных уровнях.

Масштабность проблематики кибербезопасности и степень вовлеченности к ее решению крупнейших мировых игроков побуждают к поиску решений несмотря на традиционную терминологическую и другую неопределенность, так или иначе отражает принципиальные различия по осмыслению не только проблематики кибербезопасности, но и проблематики международной безопасности в целом. Как показал анализ деятельности ООН, можно говорить о том, что даже на уровне ООН до сих пор не существует общепризнанного подхода к определению того, что считать основным предметом межгосударственных договоренностей в соответствующей сфере безопасности деятельности: страхование мирового киберпространства или обеспечения режима международной информационной безопасности.

Стоит отметить и проблемы в терминологическом аспекте. Как отмечает А.В. Демидов, концептуальной альтернативой традиционным подходам к пониманию глобальной информационной безопасности, является определение сферы проблем и угроз безопасности через понятие «кибербезопасность». Соответственно, сторонники такой концепции сужают среду угроз, с информационной, к киберпространству. Он обращает внимание и то, что проблематика кибербезопасности, прежде всего, сосредоточена на безопасности инфраструктуры компьютерных сетей, а такие вопросы, как влияние информационных потоков на социально-политические и другие процессы, не входят в проблематику кибербезопасности, таким образом, существенно сужая предмет ее регулирования[134].

Так, западные исследователи, в подавляющем большинстве случав, используют термин «кибербезопасность», под которым понимают «защиту

[134] Демидов О. В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс Безопасности. – 2013. – № 1. С. 136.

киберпространства, электронной информации, информационно-коммуникационных технологий в киберпространстве, пользователей в киберпространстве и их личностного, гражданского и национального потенциалов, включая любые их интересы, независимо от того, материальные они или нематериальные, если они уязвимы в случае нападений в киберпространстве»[135].

Одной из попыток согласования терминологии и наработки специального глоссария с переводом ключевых терминов на два языка – английский и русский в сфере МИБ, стало совместное исследование Института Запад-Восток и Института по проблемам информационной безопасности МГУ имени М. В. Ломоносова, получившее название «Российско-американский базовый перечень критических понятий в сфере кибербезопасности». Первая редакция этого глоссария появилась в 2011 году и включает в себя определение 20 терминов, которые были разделены на три блока. Первый блок содержит определения таких терминов, как: киберпространство, киберинфраструктура, киберсервисы (услуги, службы) и пр. Второй блок включает: киберпреступления, кибертерроризм, киберконфликты, кибервойны и кибербезопасность. Остановимся на определении кибербезопасности. В понимании авторов глоссария кибербезопасность – это «способность (киберпространства, киберсистемы) противостоять умышленным или непреднамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз»[136]. Третий блок включает определение таких терминов: боевые действия в киберпространстве, кибератака, оборонительные меры противодействия в киберпространстве, кибероборона, средства киберсдерживания и пр.

Ответ на вопрос, почему в глоссарии используется исключительно приставка «кибер» и мы не находим его в переводе «информационная (-ый)», содержится во введении к глоссарию, где дается краткий обзор подходов к содержательному наполнению этих понятий. Там отмечается, что с позиции

[135] Von Solms R. From information security to cyber security // Computers & security. – 2013. – Vol. 38. P. 101.
[136] Rauscher K. F., Yaschenko V. Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations // [Electronic resource] URL: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng= en&id=130080 (accessed: 13.03.2019)

российских специалистов, термин «информационный» имеет более широкое значение, исходя из того, что информация имеет две характеристики: содержательную и техническую, а термин «кибер» охватывает только ее технический аспект. Представители России понимают информационную безопасность как совокупность человеческого, социального, духовного и технического аспектов, в то время как «кибер» отражает лишь последний из них. Они подчеркивают, что защита населения от терроризма и цензуры также являются важными элементами информационной безопасности. Американские ученые не возражают против других аспектов информации, но считают ее вне предмета регулирования. Однако, американцы возражают против регулирования содержательного наполнения информации, поскольку видят в этом попытку внести цензуру в регулирование сети Интернет и попытки ограничить осведомленность населения. После консультаций было решено ограничиться термином «кибербезопасность» в узком его смысле как части «информационной безопасности», обосновывая это тем, что сейчас проблемы «кибербезопасности» требуют немедленного урегулирования[137].

Новая редакция глоссария появилась в 2014 году и была расширена до 40 терминов. Документ сохранил разделение на три блока, каждый из которых был дополнен новыми терминами. К первому блоку были добавлены такие термины, как «информационное пространство». Важным шагом стало определение понятия «международное информационное пространство», под которым понимается «любая международная среда, в которой информация создается, через которое передается, принимается, в котором хранится, обрабатывается и уничтожается»[138]. Такой подход фактически закрепил российский подход к пониманию международного информационного пространства. Ко второму блоку понятий были добавлены следующие: информационная операция, информационная война, информационный конфликт, киберугроза. Третий блок

[137] Ibid.

[138] The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations 2 / ed. J. B. Godwin III, A. Kulpin, K. F. Rauscher, V. Yaschenko // [Electronic resource] URL: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=178418&lng=en (accessed: 14.03.2019)

был пополнен определениями: информационное доминирование, информационная операция, информационная безопасность, кибероружие. Так, впервые два диаметрально разных подхода были объединены в общем смысле «международной информационной безопасности» как способности международного информационного пространства противостоять угрозам, реагировать на них и восстанавливаться (после нанесения вреда).

С учетом вышесказанного, терминологический вопрос является принципиальным, поскольку отражает несовместимые взгляды крупнейших игроков. Концептуальная ключевое отличие состоит в том, что США и значительная часть европейских государств придерживаются точки зрения о необходимости рассматривать на международном уровне только проблемы кибербезопасности, оставляя в стороне проблемы информационно-психологических воздействий. Зато такие международные акторы, как РФ, КНР последовательно отстаивают позицию, согласно которой кибербезопасность нельзя рассматривать как отдельный технико-технологическое направление, то есть обособленно от социальных, политических, экономических и военных последствий применения современных информационных технологий.

Активно к теме безопасности киберпространства обращается и Международный союз электросвязи (МСЭ), особенно после завершения «женевского» и «тунисского» форумов WSIS и Полномочной конференции МСЭ 2006 года. Ключевая роль МСЭ, по мнению руководителей этой организации, заключается в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий. Такую позицию поддерживают главы государств и правительств и другие мировые лидеры, участвовавшие во встречах под эгидой МСЭ. Они делегировали этой организации полномочия разрабатывать конкретные меры по ограничению киберугроз и незащищенности, связанных с информационным обществом.

МСЭ принял ряд резолюций и рекомендаций, которые непосредственно касающихся проблемы кибербезопасности. Особого внимания заслуживает

Рекомендация МСЭ-Т X.1205 от 2008 года[139], которая дает определение кибербезопасности, представляет в систематизированной форме угрозы кибербезопасности и уязвимости (включая перечнем самых распространенных инструментов хакерских атак). Кроме того, в Рекомендации МСЭ 2008 г. сделан обзор различных технологий кибербезопасности включая антивирусной защитой, системами обнаружения вторжений, мониторинга систем и т.п., представлены принципы защиты сетей, технологий и стратегий управления рисками и т.д. Отметим, что пока МСЭ является едва ли не единственной международной организацией, которая «осмелилась» определить понятие кибербезопасность как «набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, руководящие принципы, подходы к управлению рисками, действиями, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. При этом, ресурсы организации и пользователя включают подключены компьютерные устройства, персонал, инфраструктуру, программы, услуги, системы электросвязи и всю совокупность переданной и сохраненной информации в киберсреде. Кибербезопасность заключается в попытках достичь и сохранить свойства безопасности в ресурсах организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде»[140].

В 2016 году в Хаммамете ассамблея МСЭ-Т приняла Резолюцию – 50 «Кибербезопасность», которая привлекла внимание к необходимости более интенсивного сотрудничества членов МСЭ для выработки согласованных стандартов в борьбе с киберпреступностью, а также увеличение масштабов информирования о таких преступлениях и соответствующие механизмы противодействия[141].

---

[139]Recommendation ITU-T X.1205 (04/2008) // [Electronic resource] URL: http://handle.itu.int/11.1002/1000/9136-en (accessed: 14.03.2019)

[140] Resolution UTI 81: Definitions and terminology relating to building confidence and security in the use of information and communication technologies // [Electronic resource] URL: https://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf (accessed: 14.03.2019)

[141] Резолюция Всемирной Ассамблеи по стандартизации электросвязи № 50 – Кибербезопасность // [Электронный ресурс]. URL: https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2016-PDF-R.pdf (дата обращения: 12.03.2019)

Среди важных шагов МСЭ, направленных на дальнейшее обеспечение безопасности киберпространства, можно выделить создание специалистами этой структуры такого важного документа, как «Понимание киберпреступности: Руководство для развивающихся стран»[142]. В Руководстве изложены ключевые взгляды МСЭ на ситуацию в сфере кибербезопасности, предложены ключевые определения и универсальная модель взаимодействия основных субъектов обеспечения кибербезопасности на национальном уровне. До сих пор этот документ остается достаточно актуальным и взвешенным. Факт чрезвычайной важности проблематики кибербезопасности для МСЭ показал, что именно этот вопрос был центральным в повестке дня Пятого Всемирного форума по политике в области электросвязи, который состоялся в июне 2013 года в Женеве.

Активную политику в сфере обеспечения кибербезопасности проводит и ЕС, который на сегодняшний день объединяет высокоразвитые страны, устанавливая нормы и стандарты поведения государств в политической, экономической, социальной, информационной и иных сферах. Так, еще в 1991 г. европейские страны разработали «Европейские критерии безопасности информационных технологий»[143], которыми определялись задачи обеспечения информационной безопасности. В 1996 г. стандарты европейской информационной безопасности были воплощены в «Единые критерии безопасности информационных технологий»[144], согласно которым для характеристики основных критериев информационной безопасности применяется модель триады CIA, предусматривающая три базовые характеристики информационной безопасности: конфиденциальность, целостность и доступность[145].

---

[142] Понимание киберпреступности: Руководство для развивающихся стран 2009 г. // [Электронный ресурс]. URL: https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf (дата обращения: 14.03.2019)

[143] Information Technology Security Evaluation Criteria (ITSEC) // [Electronic resource] URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile (accessed: 14.03.2019)

[144] Common Criteria for Information Technology Security Evaluation // [Electronic resource] URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf (accessed: 14.03.2019)

[145] Ibid

В 2001 году Европейской Комиссией был представлен первый документ под названием «Сетевая и информационная безопасность: европейский политический подход»[146], в котором обозначены европейский подход к проблеме информационной безопасности. В документе используется термин «сетевая и информационная безопасность», который трактуется как способность сети или информационной системы сопротивляться случайным событиям или злонамеренным действиям, которые представляют угрозу доступности, подлинности, целостности и конфиденциальности данных, хранящихся или передаются, а также услуг, предоставляемых через эти сети и системы[147].

Стоит отметить, что руководящие документы ЕС в информационной сфере (стратегии, программы, планы) не являются неизменными, в их развитие могут приниматься новые документы, которые уточняют или дополняют предыдущие, учитывая появление новых условий или вызовов на определенном направлении. В частности, в сфере обеспечения информационной безопасности, в развитие принятой в ЕС в 2006 году. «Стратегии для безопасного информационного общества – Диалог, сотрудничество и расширение прав и возможностей»[148], Европейская Комиссия в 2013 предложила новый документ – «Стратегию кибербезопасности Европейского Союза: открытое, надежное и безопасное киберпространство»[149].

Обеспечение безопасности сетевых и информационных систем в ЕС имеет важное значение для поддержания онлайн-экономики и обеспечения процветания. Европейский Союз работает по целому ряду направлений для продвижения кибер-устойчивости в странах ЕС. Учитывая динамично развивающиеся угрозы и опираясь на обзор стратегии кибербезопасности ЕС 2013 года, совместное решение проблем кибербезопасности стало одной из трех

[146] Communication from the European Commission: "Network and Information Security: Proposal for a European Policy Approach" (COM 298 June 6, 2001 // [Electronic resource] URL: http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf (accessed: 14.03.2019)
[147] Ibid
[148] A strategy for a Secure Information Society – Dialogue, partnership and empowerment // [Electronic resource] URL: http://ec.europa.eu/information_society/doc/com2006251.pdf (accessed: 15.03.2019)
[149] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // // [Electronic resource] URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed: 15.03.2019)

задач, выявленных в среднесрочном обзоре единого цифрового рынка. Еврокомиссия и Высший представитель предложили широкий спектр конкретных мер, которые позволят укрепить структуры кибербезопасности ЕС при расширении сотрудничества между государствами-членами и различными структурами ЕС.

13 сентября 2017 года Европейская Комиссия приняла пакет мер по кибербезопасности. Документ опирается на существующие нормативно-правовые и создает новые инициативы по дальнейшему повышению устойчивости кибербезопасности ЕС.

Ниже приведены некоторые из мер:

- Повысить устойчивость к кибер-атакам. В Евросоюзе было создано агентство по сетевой и информационной безопасности, играющее ключевую роль – ENISA.

Комиссия предлагает реформу, чтобы ЕНИСА могла оказывать поддержку государствам-членам, учреждениям ЕС и деловым кругам в ключевых областях, включая осуществление Директивы по безопасности сетевых и информационных систем[150]. Это будет способствовать сотрудничеству и урегулированию кризисов в рамках ЕС.

- Единый рынок кибербезопасности. Рост рынка кибербезопасности в ЕС, с точки зрения создания новых продуктов и услуг сдерживается несколькими способами, в том числе из-за отсутствия признанной во всем ЕС системы сертификации кибербезопасности. Поэтому Комиссия выдвигает предложение о создании системы сертификации в ЕС, в основе которой лежит ЕНИСА.

- Директива NIS (Директива (ЕС) N 2016/1148)[151]

Необходимо оперативное выполнение директивы NIS (Директива о безопасности сетевых и информационных систем), принятой в июле 2016 года.

[150] Directive of the European Parlament of 6 July 2016 Concerning measures for a high common level of security of network and information systems across the Union // [Electronic resource] URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (accessed: 15.03.2019)

[151] Proposal for a Directive of the european parliament and of the council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision // [Electronic resource] URL: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-489_en (accessed: 15.03.2019)

Выполнению Директивы способствует руководство Комиссии по практическому применению Директивы и дополнительная интерпретация конкретных положений, включенных в пакет положений сентября 2017 года. Директива определяет и устанавливает требования, направленные на обеспечение высокого уровня информационной безопасности сетей и информационных систем на территории ЕС. Ее действие распространяется на операторов критической инфраструктуры, в том числе, на крупные банки и другие компании, вовлеченные в финансовую торговлю, операторов энергоснабжения, нефтяных и газовых сетей; а также на те организации, которые осуществляют контроль за системами воздушного, автомобильного и железнодорожного транспорта; организации, осуществляющими свою деятельность в сфере здравоохранения; компании, контролирующих водоснабжение; а также операторов цифровых инфраструктур и «поставщиков цифровых услуг» (интернет-биржи, поисковые системы, облачные сервисы и т.д.)

- Правила обработки персональных данных в Европе (GDPR)

Вступила в силу 15 мая 2018 года. Данный регламент предоставляет странам-членам ЕС полный контроль за своими персональными данными. Кроме того, ожидается ужесточение штрафов за нарушения правил хранения персональных данных: до 20 млн евро или 4% ВВП. Таким образом, данный документ является гарантом защиты персональных данных в ЕС и за его пределами. Данная реформа усиливает существующие правила в отношении вопросов защиты персональных данных, а также расширяет возможности граждан в отношении контроля за их собственными персональными данными.

- План быстрого реагирования на чрезвычайные ситуации

Комиссия представила план, хорошо отрепетированный в случае крупномасштабного трансграничного кибер-инцидента или кризиса. В нем излагаются цели и способы сотрудничества между государствами-членами и учреждениями ЕС реагирования на такие инциденты, а также разъясняется, каким образом существующие механизмы управления кризисами могут в полной

мере использовать существующие структуры кибербезопасности на уровне ЕС[152].

Согласно отчету Европейской комиссии[153], за 2017 год, европейцы считают, что цифровые технологии позитивно влияют на три сферы: экономику (35%), общество (33%), качество жизни (32%). Кроме того, такие секторы экономики как: транспорт, энергетика, здравоохранение и финансы становятся все более зависимыми от сети и информационных систем. В ежегодном отчете особо выделяется, что Интернет вещей - это уже реальность. Согласно подсчетам, к 2020 году будут подключены десятки миллиардов цифровых устройств только лишь в Евросоюзе[154].

Что же касается Североатлантического Альянса, то основным принципом информационной безопасности НАТО является то, что информация должна сохранять свою степень защиты при всех ее передачах, начиная с источника, а контроль за распределением и распространением информации должен обеспечить отсутствие ее утечки, а также и то, что правила доступа к информации должны разрешать использование информации только лицам, которым она нужна для выполнения служебных обязанностей. Присвоение информации НАТО того или иного грифа секретности производится в соответствии с правилами систем безопасности стран-участниц.

Большинство стран ЕС являются членами НАТО, соответственно, на них распространяются такие ключевые документы Альянса в сфере кибербезопасности, как: стандарты НАТО по защите информации, изложенные в документе СМ (2002) «Безопасность в организации Североатлантического

[152] Меры по обеспечению кибербезопасности ЕС // [Электронный ресурс]. URL: https://ec.europa.eu/digital-single-market/en/policies/cybersecurity (дата обращения: 10.03.2019)
[153] PWC, Global State of Information Security Survey, 2016 // [Electronic resource] URL: http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/. (accessed: 10.03.2019)
[154] Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, IDC and TXT, study carried out for the European Commission, 2014 // [Electronic resource] URL: http://publications.europa.eu/resource/cellar/35f3eccd-f7ce-11e5-b1f9-01aa75ed71a1.0001.01/DOC_1 (accessed: 10.03.2019)

договора (НАТО)»[155], официальная политика НАТО в сфере киберзащиты[156], стратегическая концепция кибербезопасности, сформулированная по результатам Лиссабонского саммита[157] и уточненная по результатам Варшавского саммита[158] и пр.

Как было отмечено в стратегическом исследовании группы экспертов НАТО, организация должна ускорить свою деятельность по реагированию на опасность кибератак, защищая собственные системы связи и управления, помогая союзникам по Альянсу усовершенствовать свою способность предотвращать нападения и восстанавливаться после них, и развивать силы и средства киберзащиты с целью эффективного выявления и сдерживания кибернетических атак[159].

Основной передовой опыт НАТО в области кибербезопасности – Объединенный центр в сфере кибероборонь НАТО, сформированный в 2008 г. в г. Таллин. Основной задачей центра является обучение и консультирование специалистов, проведение исследований в сфере кибербезопасности[160]. Данный Центр является флагманом европейской кибербезопасности: он имеет аккредитацию НАТО – формально не входя в командную структуру, он имеет огромное влияние на действия НАТО по защите от киберугроз. Центр основали семь стран, а на сегодняшний день он насчитывает 20 участников – 17 членов НАТО и 3 страны-партнера. Уникальность центра заключается в том, что там вместе работают военные, гражданские лица и представители правительства. Работа центра сфокусирована на трех основных направлениях: исследование, тренировки и обучение. Надо подчеркнуть, что данный центр не является

---

[155] Security within the North Atlantic Treaty Organization C-M(2002)49 // [Electronic resource] URL: http://www.freedominfo.org/documents/C-M(2002)49.pdf (accessed: 10.03.2019)

[156] NATO Bucharest Summit Declaration 3 April 2008 // [Electronic resource] URL: https://www.nato.int/cps/ua/natohq/official_texts_8443.htm (accessed: 10.03.2019)

[157] NATO Lisbon Summit Declaration 20 Nowember 2010 // [Electronic resource] URL: https://www.nato.int/cps/en/natohq/official_texts_68828.htm (дата обращения: 10.03.2019)

[158] NATO Warsaw Summit Communiqué, 9 July 2016 // [Electronic resource] URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed: 10.03.2019)

[159] John E Dunn. NATO clause V could deter cyberattack, says defence minister // [Electronic resource] URL: https://www.networkworld.com/article/2194246/security/nato-clause-v-could-deter-cyberattack--says-defence-minister.html (accessed: 07.03.2019)

[160] Смирнов А.И. Современные информационные технологии в международных отношениях: монография. - М.: МГИМО-Университет, 2017. С. 248.

операционным подразделением по борьбе с хакерами, хотя в нем проходят тренировки специалистов из разных стран, которые затем обеспечивают национальную кибербезопасность, а также делятся информацией с НАТО и партнерами.

В 2015 г. в Таллинне был создан Кибернетический тренировочный центр НАТО – виртуальная среда, что позволяет проводить тренинги специалистов, отрабатывать индивидуальные и командные навыки. Так с 2015 г. центром ежегодно проводит крупнейшие в мире киберучения «Locked Shields» для экспертов в области киберзащиты[161]. На учениях модулируют нападения на реальные объекты и задействуют те же протоколы, как и в случае настоящей атаки.

Весной 2013 г. Центр опубликовал «Таллиннское руководство» по вопросам применения положений и норм международного права к условиям различных конфликтов в киберпространстве. Ряд положения документа санкционирует применение широкого спектра кинетического оружия против источников киберугроз, силовые действия в отношении лиц, которые причастны к кибератакам, а также военные кибероперации, направленные против критической информационной инфраструктуры. В 2017 году вышло расширенное «Таллиннское руководство 2.0». Это издание дополнило уже существующие пункты, но основные положения остались неизменными. Стоит обратить внимание на небольшое изменение в названии. В первой редакции название было «Таллинское руководство по ведению кибервойн», а во второй название поменяли на «Таллинское руководство по проведению кибероперацій». Данное изменение показывает, что Таллинское руководство может являтся прототипом международного права в киберпространстве и в будущем может лечь в основу такого права. Также Центр ведет работу над доктриной по киберзащите в качестве единственного алгоритма действий,

[161] Locked Shields 2017 // [Electronic resource] URL: https://ccdcoe.org/locked-shields-2017.html (accessed: 07.03.2019)

которого могли бы придерживаться страны в случае нападения[162]. В апреле 2019 Центр провел крупнейшие в мире киберучения. Согласно сценарию учений Locked Shields 2019, Центр приступил к отражению кибератак на несуществующее государство «Берилия».

В сети центров передового опыта НАТО важное место отводится Центру в области стратегических коммуникаций (Страткому), начавшему свою работу в начале 2014 г. и получившего аккредитацию в сентябре того же года. Открытие данного центра произошло в августе 2015 г., на котором была выражена точка зрения семи членов НАТО о том, что Центр призван побеждать противников при помощи наиболее современных ИКТ. Утверждалось, что в арсенале Центра «имеются все необходимые средства, способные заставить врагов потерять волю к победе и возненавидеть собственную страну, что приведет к победе»[163].

Также в преддверии Варшавского саммита 2016 г. НАТО совместно с ЕС подписали документ о сотрудничестве в борьбе с угрозами кибербезопасности, где отмечается, что ЕС и НАТО намерены совместно анализировать, работать над предупреждением и обнаружением всяческих гибридных угроз, своевременно обмениваться информацией и разведывательными данными[164]. В Финляндии с сентября 2017 работает Европейский центр противодействия гибридным угрозам. Решение о создании финского Центра было принято в апреле 2017 представителями стран НАТО и ЕС, учредителями центра стали 12 страна стартовый бюджет составил около 2 млн. евро[165]. Основными целями центра стало повышение осведомленности членов ЕС в области противостояния гибридным угрозам и их способности бороться с ними, а также усиление сотрудничества с органами НАТО, которые специализируются на

[162] Tallinn Manual on the International Law Applicable to Cyber Warfare / ed. Schmitt M. - Cambridge University Press, 2013.

[163] Центр пропаганды НАТО в Риге выиграет войну без единого выстрела // [Электронный ресурс]. URL: https://russian.rt.com/inotv/2015-08-21/PBK-Centr-propagandi-NATO-v (дата обращения: 12.03.2019)

[164] НАТО-ЕС: Декларация о сотрудничестве // [Электронный ресурс]. URL: http://ru.euronews.com/2016/07/08/nato-and-the-eu-have-signed-a-deal-aimed-at-boosting-cooperation-on-defence (дата обращения: 12.03.2019)

[165] European Centre of Excellence for Countering Hybrid Threats officially opens in Helsinki // [Electronic resource] URL: https://www.urm.lt/default/en/news/european-centre-of-excellence-for-countering-hybrid-threats-officially-opens-in-helsinki (accessed: 12.03.2019)

противодействии таким угрозам (сотрудничество с Таллиннским и Рижским центрами).

Помимо тройки центров, также стоит отметить и технический центр Сил реагирования НАТО на компьютерные инциденты NCIRC, который стал мозговым узлом борьбы Альянса против киберпреступности. Так, NCIRC отвечает за киберзащиту всех информационных ресурсов НАТО, независимо от того, принадлежат они постоянным штабам, или штабам, развернутым на время операций или учений. В начале 2012 года НАТО подписала контракт стоимостью 67 млн. долл. США с итальянской компанией Finmeccanica на разработку, внедрение и обслуживание программы киберзащиты NCIRC. В рамках соглашения итальянская компания при поддержке американской, обеспечивает информационную безопасность примерно 30 важным объектам и штабквартиру НАТО в 28 странах мира[166]. NCIRC достиг полной оперативной готовности уже в начале 2013 года, когда были разработаны и условия сотрудничества, в том числе между экспертами, которые пользуются взаимным доверием и представляют страны, промышленность, академические круги и НАТО. Эти договоренности наконец открыли доступ к специальным знаниям во всех сферах кибербезопасности. Разработаны также и требования к экспертам, участвующим в миссиях по оказанию помощи, где определяются сферы их компетенции. Все процедуры Группы быстрого реагирования НАТО и возможные действия определены в руководстве, над которым постоянно продолжают работать эксперты в области противодействия киберпреступности и специалисты по планированию на случай чрезвычайных ситуаций гражданского характера. В этом пособии закреплено рекомендации по реагированию НАТО по просьбе государств-членов и партнеров о помощи в защите их информационных и коммуникационных систем.

Таким образом, можно говорить о том, что на сегодняшний день глобальные мировые акторы осознают прямую зависимость своего

[166] NATO Rapid Reaction Team to fight cyber attack // [Electronic resource] URL: https://www.nato.int/cps/uk/natohq/news_85161.htm?selectedLocale=en (accessed: 12.03.2019)

благосостояния от информационной сферы, поэтому вопрос обеспечения кибербезопасности закономерно занимает одно из ведущих мест в ведущих документах ЕС, НАТО и соответствующих государств. В то же время политика обеспечения информационной безопасности большинства стран имеет проактивный характер и опирается на принципы управления рисками информационной безопасности, прежде всего – кибербезопасности. Страны-члены НАТО аналогично считают решение проблемы обеспечения кибербезопасности, в контексте личности, общества, государства, их защиты от внутренних и внешних, в том числе гибридных угроз, одним из самых важных стратегических приоритетов обеспечения национальной безопасности.

ЗАКЛЮЧЕНИЕ

На основании проведенного исследования, мы можем сделать следующие выводы:

1. Одним из универсальных факторов международных отношений является глобальная безопасность, которая также включает в себя безопасность информационную и кибербезопасность. В деятельности международного сообщества, а также при формировании национальных внешних векторов стран, этот фактор приводит к радикальным изменениям поведения акторов международных отношений и трансформации сущности безопасности. Стоит вспомнить те изменения в контексте безопасности, проходившей после окончания «холодной войны» и краха биполярной системы. В постбиполярном мире возникла необходимость новых принципов работы институтов в сфере безопасности, как на национальном, так и на международном уровне с учетом информационной составляющей. С появлением новых вызовов и угроз в информационной сфере осложняется сама структура международных отношений. Вместе с тем, информационная среда является одним из важнейших факторов развития человечества, которая отражает, как потребность, так и специфику современной цивилизации, связанной с достижениями и вызовами развития государств, общества и личности.

2. На основании рассмотрения исследовательских точек зрения, считаем необходимым понимать под киберпространством виртуальную коммуникационную среду, образованную системой связей между пользователями и объектами информационной инфраструктуры, такими как электронный информационный ресурс, системы и сети всех форм собственности, управляемые автоматизированными системами управления, которые используются не только для преобразования и передачи информации, которая в них циркулирует, с целью обеспечения информационных потребностей общества, но и для влияния на аналогичные объекты противоборствующей стороны.

3. На сегодняшний день киберпространство в своей непосредственной совокупности является важным составным элементом всей повседневной жизни современного общества в целом и отдельного человека в частности. Долгое время киберпространство воспринималось большинство мировых акторов, в качестве непосредственного внутриполитического вопроса, а сам термин использовался для непосредственного обозначения определенного фона (фоновых условий), перманентных процессов и решений в рамках тех или иных процессов. Закономерным видится также допущение о том, что в отличие от внутренней политики государства, киберпространство имеет характерные черты и области взаимодействия с внешним миром, что частично попадает в сферу влияния внешней политики и также затрагивает элементы национальной безопасности, включая основные институты и системы принятия решений, каждая из которых имеет важное значение для государства, государственных интересов во внешней и внутренней политике государства в каждый отдельный промежуток времени. Иными словами, на сегодняшний день киберпространство последовательно формирует область внешней политики, тогда как непосредственно внешняя политика формирует будущее государства. В данном контексте, сфера международных отношений, которая уходит своим и корнями в теории и проблемы прошлого, следует допустить, не всегда и не в полной мере может успевать за возрастающим значением киберпространства и трансформации роли данного фактора, его важности для международных отношений в целом.

4. Использование современных информационно-коммуникационных технологий, без сомнения, выходит за рамки национальной безопасности, так как нуждается в применении действенных механизмов по противодействию угрозам в киберпространстве. Любая кибератака начинается с использования ИКТ, однако может очень быстро выйти за рамки виртуальной среды, создавая угрозу экономике, бизнес-среде, государству и индивидам в целом. В данной связи обеспечение кибербезопасности и информационной безопасности в целом, является одним из приоритетных направлений деятельности не только

государств, но и региональных объединений, координации усилий всего международного сообщества. Это тот приоритет, который, фактически, объединяет континенты, государства и международные организации. Несмотря на успешный опыт отдельных государств, а также определенные позитивные сдвиги в направлении международного сотрудничества в области кибербезопасности на уровне ООН, ЕС, НАТО, важно не останавливаться на достигнутых результатах, так как информационные коммуникации продолжают стремительно развиваться, аналогично, как и увеличивается количество киберугроз и сфера их распространения. Международное сотрудничество по кибербезопасности должно обладать системным и последовательным характером, сопровождаться основательными исследованиями, в особенности это касается предупреждения и устранения угроз кибербезопасности.

5. В особенности, важно решить несколько принципиальных осложнений (прежде всего на международном уровне), которые делают невозможным формализацию безопасности в киберпространстве:

- до сих пор отсутствуют системные международные нормативно-правовые документы, которые четко бы давали определение киберпространства и всех производных от него элементов, характерный безопасности;

- не определен правовой статус киберпространства;

- отсутствует консенсус на международном уровне о правилах поведения в киберпространстве;

- отсутствует общепринятая методология оценки последствий киберпреступлений и их привязка к международным нормам и правилам (в частности, о признании кибератаки как акта войны).

6. Подытоживая, отметим, что формирование сектора кибербезопасности, как на национальном, так и международном уровнях продолжается. Этот процесс сталкивается с рядом проблем, обусловленных инновационным характером проблематики киберпространства. Сущностными проблемами становятся терминологическая неопределенность и неготовность действующей международно-правовой базы дать ответ на новые угрозы. Отдельные усилия

(вроде принятия «Конвенции о киберпреступности») остаются лишь ограниченно успешными из-за неготовности всех стран полноценно присоединиться к ним. Дополнительной проблемой становится концептуальное расхождение взглядов основных геополитических игроков на природу и правила поведения в киберпространстве. Ощущается нехватка методологических подходов для адаптации кибератак к действующей нормативно-правовой базе. Предложенные отдельными учеными методологические рамки представляют значительный интерес, однако остаются фрагментарными. Растущая активность сторонников «радикального» подхода к кибератакам (когда они понимаются как «акт войны» с соответствующими последствиями) позволяет предположить, что тема кибератак и кибервойны в дальнейшем будет находиться в центре внимания дискуссий мировых геополитических игроков.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Источники:

1. Венская декларация о преступности и правосудии: ответы на вызовы XXI века. Принята на Десятом Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, Вена, 10 – 17 апреля 2000 года // [Электронный ресурс] URL: http://www.un.org/ru/documents/decl_conv/declarations/vendec.shtml (дата обращения: 04.03.2019)
2. Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии 12 декабря 2003 г. // [Электронный ресурс]. URL: http://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения: 07.03.2019)
3. Дохинская декларация о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку дня Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности от 19 апреля 2015 г. // [Электронный ресурс] URL: https://www.unodc.org/documents/congress/Declaration/V1504153_Russian.pdf (дата обращения: 11.03.2019)
4. Окинавская хартия Глобального информационного общества от 21 июля 2000 г. // [Электронный ресурс] URL: http://www.kremlin.ru/supplement/3170 (дата обращения: 28.02.2019)
5. Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г.: Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // [Электронный ресурс]. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 02.03.2019)
6. Резолюция Генеральной Ассамблеи ООН 55/63 от 22 января 2001 г.: Борьба с преступным использованием информационных технологий // [Электронный ресурс]. URL: http://www.ifap.ru/ofdocs/un/5563.pdf (дата обращения: 04.03.2019)
7. Резолюция Генеральной Ассамблеи ООН 56/19 от 7 января 2002 г.: Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // [Электронный ресурс]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement (дата обращения: 07.03.2019)

8. Резолюция Генеральной Ассамблеи ООН от 23 декабря 2003 г.: Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур // [Электронный ресурс]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/54/PDF/N0350654.pdf?OpenElement (дата обращения: 08.03.2019)

9. Резолюция ГА ООН A/RES/65/230 «Сальвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире» // [Электронный ресурс] URL: http://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration.shtml (дата обращения: 08.03.2019)

10. Резолюция Всемирной Ассамблеи по стандартизации электросвязи № 50 – Кибербезопасность // [Электронный ресурс]. URL: https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2016-PDF-R.pdf (дата обращения: 12.03.2019)

11. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН 56/121 от 23 января 2002 [Электронный ресурс]. URL: //www.un.org/russian/documen/gadocs/56sess/56reslis.htm (дата обращения: 07.03.2019)

12. Всемирная встреча на высшем уровне по вопросам информационного общества // [Электронный ресурс]. URL: http://www.un.org/ru/events/pastevents/wsis.shtml (дата обращения: 08.03.2019)

13. Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями (Вена, 10–17 апреля 2000 г.) Преступления, связанные с использованием компьютерной сети: справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети // [Электронный ресурс] URL: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_R.pdf (дата обращения: 04.03.2019)

14. Доклад о работе двенадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию (12–19 апреля 2010 г.) // [Электронный ресурс] URL: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053830r.pdf (дата обращения: 08.03.2019)

15. Инициатива стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» // [Электронный

ресурс]. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/916241 (дата обращения: 12.03.2019)

16. Понимание киберпреступности: Руководство для развивающихся стран 2009 г. // [Электронный ресурс]. URL: https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf (дата обращения: 14.03.2019)

17. Развитие и международное сотрудничество в XXI веке: роль информационной технологии в контексте основанной на знаниях глобальной экономики : Декларация министров на этапе заседания ЭКОСОС высокого уровня, принятая Экономическим и Социальным Советом от 7 июля 2000 года // [Электронный ресурс] URL: http://www.un.org/ru/development/ict/ecosoc_decl2000.htm (дата обращения: 04.03.2019)

18. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. // [Электронный ресурс]. URL: http://www.mid.ru/foreign_policy/international_contracts/2_contract/-/storage-viewer/bilateral/page-38/43921 (дата обращения: 12.03.2019)

19. Концепция стратегии кибербезопасности Российской Федерации (проект) // [Электронный ресурс] URL: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 09.03.2019).

20. «Лаборатория Касперского» раскрыла шпионскую сеть «Red October» // [Электронный ресурс]. URL: http://24gadget.ru/1161053174-laboratoriya-kasperskogo-raskryla-shpionskuyu-set-red-october.html (дата обращения: 11.03.2019).

21. Международное сотрудничество в области информационной безопасности // [Электронный ресурс]. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/486848 (дата обращения: 04.03.2019)

22. Меры по обеспечению кибербезопасности ЕС // [Электронный ресурс]. URL: https://ec.europa.eu/digital-single-market/en/policies/cybersecurity (дата обращения: 10.03.2019)

23. НАТО-ЕС: Декларация о сотрудничестве // [Электронный ресурс]. URL: http://ru.euronews.com/2016/07/08/nato-and-the-eu-have-signed-a-deal-aimed-at-boosting-cooperation-on-defence (дата обращения: 12.03.2019)

24. Центр пропаганды НАТО в Риге выиграет войну без единого выстрела // [Электронный ресурс]. URL: https://russian.rt.com/inotv/2015-08-21/PBK-Centr-propagandi-NATO-v (дата обращения: 12.03.2019)

25. A strategy for a Secure Information Society – Dialogue, partnership and empowerment // [Electronic resource] URL: http://ec.europa.eu/information_society/doc/com2006251.pdf (accessed: 15.03.2019)

26. 13 Alarming Cyber Security Facts and Stats // [Electronic resource] URL: https://www.cybintsolutions.com/cyber-security-facts-stats/ (accessed: 09.03.2019)

27. Common Criteria for Information Technology Security Evaluation // [Electronic resource] URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf (accessed: 14.03.2019)

28. Communication from the European Commission: "Network and Information Security: Proposal for a European Policy Approach" (COM 298 June 6, 2001 // [Electronic resource] URL: http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf (accessed: 14.03.2019)

29. Convention on Cybercrime. Budapest, 23 November 2001 // [Electronic resource] URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (accessed: 02.03.2019)

30. Cyberspace. United States Faces Challenges in Addressing Global Cybersecurity and Governance / Washington, July 2010 // [Electronic resource] URL: https://www.gao.gov/assets/310/308401.pdf(accessed: 02.03.2019)

31. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // // [Electronic resource] URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed: 15.03.2019)

32. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space // [Electronic resource] URL: http://www.officialdocuments.gov.uk/document/cm76/7642/7642.pdf (accessed: 28.02.2019)

33. Cyber Attacks During The War on Terrorism: A Predictive Analysis September 22, 2001 // [Electronic resource] URL: http://www.ists.dartmouth.edu/docs/cyber_a1.pdf (accessed: 05.03.2019)

34. Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, IDC and TXT, study carried out for the European Commission, 2014 // [Electronic resource] URL: http://publications.europa.eu/resource/cellar/35f3eccd-f7ce-11e5-b1f9-01aa75ed71a1.0001.01/DOC_1 (accessed: 10.03.2019)

35. Digital Europe: Pushing the frontier, capturing the benefits / McKinsey Global Institute. June 2016 [Electronic resource] URL:

https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20europe%20pushing%20the%20frontier%20capturing%20the%20benefits/digital-europe-full-report-june-2016.ashx (accessed: 01.03.2019)

36. Directive of the European Parlament of 6 July 2016 Concerning measures for a high common level of security of network and information systems across the Union // [Electronic resource] URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (accessed: 15.03.2019)

37. European Centre of Excellence for Countering Hybrid Threats officially opens in Helsinki // [Electronic resource] URL: https://www.urm.lt/default/en/news/european-centre-of-excellence-for-countering-hybrid-threats-officially-opens-in-helsinki (accessed: 12.03.2019)

38. GAO-10-628. Key Private and Public Cyber Expectations Need to Be Consistently Addressed / United States Government Accountability Office, Washington, July 2010 // [Electronic resource] URL: https://www.gao.gov/assets/310/307222.pdf (accessed: 02.03.2019)

39. Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019 // [Electronic resource] URL: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 (accessed: 08.03.2019)

40. German Cyber Security Strategy // [Electronic resource] URL: http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy2011-1 (accessed: 28.02.2019)

41. Hackers Attack Every 39 Seconds / Security. February 10, 2017 [Electronic resource] URL: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds (accessed: 09.03.2019)

42. Information Technology Security Evaluation Criteria (ITSEC) // [Electronic resource] URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile (accessed: 14.03.2019)

43. Locked Shields 2017 // [Electronic resource] URL: https://ccdcoe.org/locked-shields-2017.html (accessed: 07.03.2019)

44. National Military Strategy for Cyberspace Operations // [Electronic resource] URL: http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.%20pdf (accessed: 28.02.2019)

45. NATO Bucharest Summit Declaration 3 April 2008 // [Electronic resource] URL: https://www.nato.int/cps/ua/natohq/official_texts_8443.htm (accessed: 10.03.2019)

46. NATO Lisbon Summit Declaration 20 Nowember 2010 // [Electronic resource] URL: https://www.nato.int/cps/en/natohq/official_texts_68828.htm (дата обращения: 10.03.2019)

47. NATO Warsaw Summit Communiqué, 9 July 2016 // [Electronic resource] URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed: 10.03.2019)

48. NATO Rapid Reaction Team to fight cyber attack // [Electronic resource] URL: https://www.nato.int/cps/uk/natohq/news_85161.htm?selectedLocale=en (accessed: 12.03.2019)

49. Proposal for a Directive of the European parliament and of the council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision // [Electronic resource] URL: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-489_en (accessed: 15.03.2019)

50. PWC, Global State of Information Security Survey, 2016 // [Electronic resource] URL: http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/. (accessed: 10.03.2019)

51. Recommendation ITU-T X.1205 (04/2008) // [Electronic resource] URL: http://handle.itu.int/11.1002/1000/9136-en (accessed: 14.03.2019)

52. Security within the North Atlantic Treaty Organization C-M(2002)49 // [Electronic resource] URL: http://www.freedominfo.org/documents/C-M(2002)49.pdf (accessed: 10.03.2019)

53. Tackling the Challenges of Cyber Security / ETSI White Paper No. 18. December 2016 [Electronic resource] URL: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp18_CyberSecurity_Ed1_FINAL.pdf (accessed: 27.02.2019)

54. U.S. Presidential Decision Directive/ NSC-63. May 22, 1998 // [Electronic resource] URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm (accessed: 07.03.2019)

Литература:

55. Авчаров И.В. Борьба с киберпреступностью // Информатизация и информационная безопасность правоохранительных органов: Сб. ст. XI межд. науч.-прак. конф. - М., 2012. - С. 191-194.

56. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. - 2014. - № 5. - С. 39-42.

57. Антонос Г. А. Международные изменения права киберпространства // Право и информатизация общества: сб. науч. тр. - М.: ИНИОНРАН, 2012.- С. 174-186.

58. Бескоровайный М.М., Татузов А.Л. Кибербезопасность - подходы к определению понятия // Журнал Вопросы кибербезопасности. – 2014. - №1. - С. 22-27.

59. Букин Д.А. Underground киберпространства // Рынок ценных бумаг. 2013. - № 8. - С. 104 - 108.

60. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. - 2015. - № 13. - С. 96-99.

61. Бураева Л.А. Информационные войны и информационный терроризм в современном мире: методы и поле действия // Известия Кабардино-Балкарского научного центра РАН. - 2014. - № 1. - С. 7-11.

62. Бурячок В.Л. Информационная и кибербезопасность: социотехнические аспект: учебник / под общ. ред. В.Б. Толубко. - К.: ДУТ, 2015. - 288 с.

63. Галий А.А. Слюсарь И.В. «Даркнет» как угроза национальной безопасности Российской Федерации // Вестник науки. - 2018. - № 9. - С. 204-205.

64. Демидов О. В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс Безопасности. – 2013. – № 1. - С. 129-168.

65. Джаббарова К.Ф. Современные аспекты кибербезопасности в мире в контексте глобальных угроз // АНИ: Экономика и управление. - 2017. - №. 2. - С. 323-326.

66. Дубов Д.В., Ожеван М.А. Кибербезопасность: мировые тенденции и вызовы. - К.: НИСИ, 2011. - 30 с.

67. Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: монография. - М., 2016. - 168 с.

68. Згоба А.И., Маркелов Д.В. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. - 2014. - № 5. - С. 30-38.

69. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы: дис. ... докт. наук: 23.00.04. - М., 2017. – 332 с.

70. Информационные вызовы национальной и международной безопасности / Под общ. ред. Федорова А.В., Цыгичко В.Н. М.: ПИР-Центр, 2001. - 328 с.

71. Компьютерная преступность и кибертерроризм / под ред. В.А. Голубева, Э.В. Рыжкова. - Центр исслед. компьютерной преступности, 2005. (Вып. 3). - 448 с.

72. Кузнецов С. Кибербезопасность в 21 веке // [Электронный ресурс] URL: https://www.osp.ru/os/2013/05/13036002/ (дата обращения: 09.03.2019)

73. Савин Л.В. Введение в кибергеополитику // Геополитика. Информационно-аналитическое издание. Выпуск XXII, 2013. - 118 с.

74. Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности // [Электронный ресурс] URL: http://book.itep.ru/10/2012.htm (дата обращения: 04.03.2019)

75. Смирнов А.И. Современные информационные технологии в международных отношениях: монография. - М.: МГИМО-Университет, 2017. – 334 с.

76. Старостина Е. Терроризм и кибертерроризм — новая угроза международной безопасности // [Электронный ресурс] URL: http://www.crime-research.ru/articles/starostina/3 (дата обращения: 04.03.2019)

77. Супертерроризм: новый вызов нового века / Научный записки ПИР-Центра // Под общей редакцией Федорова А.В. - М. : Изд-во «Права человека», 2002. - С. 92-109.

78. Харченко В.П. Кибертерроризм на авиационном транспорте / // Проблемы информатизации и управления: Сб. науч. Трудов. Вып. 4., 2009. - С. 131-140.

79. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: Автореф. дисс. ... канд. юрид. наук: 12.00.12. - М., 2016. - 29 с.

80. Шеломенцев В.П. Концепции законопроекта о кибернетической безопасности // Борьба с Интернетпреступностью: материалы междунар. научно-техн. конф., 2013. - С. 12-14.

81. Arquilla J., Ronfeldt D. Networks and netwars: The future of terror, crime, and militancy. Rand Corporation. 2001 // [Electronic resource] URL: https://www.rand.org/pubs/monograph_reports/MR1382.html (accessed: 06.03.2019)

82. Bendovschi A. Cyber-Attacks – Trends, Patterns and Security Countermeasures // Procedia Economics and Finance. 2015. [Electronic resource] URL: https://www.researchgate.net/publication/283967866_Cyber-Attacks_-_Trends_Patterns_and_Security_Countermeasures (accessed: 07.03.2019)

83. Clark D. Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, 12 March 2010 // [Electronic resource] URL: https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf (accessed: 27.02.2019)

84. Choucri N., Goldsmith D. Lost in cyberspace: harnessing the Internet, international relations, and global security // Bulletin of the Atomic Scientists. – 2012. – Vol. 68. – P. 70-77.

85. Cohen A. The Willie Sutton Theory of Cyber Security // [Electronic resource] URL: https://www.illumio.com/blog/willie-sutton-cyber-security#gsc.tab=0 (accessed: 10.03.2019)

86. Duić I., Cvrtila V. International cyber security challenges // MIPRO. 2017. [Electronic resource] URL: https://bib.irb.hr/datoteka/878827.Duic_Cvrtila_Ivanjko_International_cyber_security_challenges_.pdf (accessed: 07.03.2019)

87. Fischer E. Cybersecurity Issues and Challenges: In Brief // [Electronic resource] URL: https://fas.org/sgp/crs/misc/R43831.pdf (accessed: 24.02.2019)

88. Fountain J. E. Building the virtual state: Information technology and institutional change. - Brookings Institution Press, 2001. - 256 p.

89. Gerald B.F. The theory the intersectionality can make cyber security collaboration real // [Electronic resource] URL: https://techcrunch.com/2015/02/17/the-theory-of-intersectionality-can-make-cybersecurity-collaboration-real/ (accessed: 08.03.2019)

90. Goutam R. Importance of Cyber Security // International Journal of Computer Applications. - 2015 . - Vol. 7. - P. 14-17.

91. Graham D. Cyber Threats and the Law of War // Journal of National Security Law & Policy. - 2010. - Vol. 4. - P. 87-102.

92. Hansen L., Nissenbaum H. Digital Disaster, Cyber Security and the Copenhagen School. University of Copenhagen, New York University // International Studies Quarterly. - 2009. - № 53. - P. 1155-1175.

93. Henry A. Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry // [Electronic resource] URL: https://unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdfRequirements (accessed: 10.03.2019)

94. ISO/IEC 27032, Information technology. Security techniques. Guidelines for cybersecurity, 2012. - 50 p.

95. John E Dunn. NATO clause V could deter cyberattack, says defence minister // [Electronic resource] URL: https://www.networkworld.com/article/2194246/security/nato-clause-v-could-deter-cyberattack--says-defence-minister.html (accessed: 07.03.2019)

96. Keith A. Warfighting in Cyberspace // [Electronic resource] URL: http://www.carlisle.army.mil/DIME/documents/Alexander.pdf (accessed: 01.03.2019)

97. Korff D. Cyber Security definitions - a selection // [Electronic resource] URL: https://www.sbs.ox.ac.uk/cybersecurity-

capacity/system/files/CPDP%202015%20-%20KORFF%20Handout%20-%20DK150119.pdf (accessed: 22.02.2019)

98. Libicki M. Crisis and Escalation in Cyberspace // [Electronic resource] URL: https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf (accessed: 07.03.2019)

99. Lih A. A virtual necessity: some modest steps toward greater cybersecurity // Bulletin of the Atomic Scientists. - 2012. - Vol. 68. - № 5. - P. 75-87.

100. Menashri H., Baram G. Critical Infrastructures and their Interdependence in a Cyber Attack –The Case of the U.S. // Military and Strategic Affairs. – 2015. – Vol. 7, №. 1. – P. 99-100.

101. Osborne Ch. Carbanak hacking group steal $1 billion from banks worldwide // [Electronic resource] URL: https://www.zdnet.com/article/carbanak-hacking-group-steal-1-billion-from-banks-worldwide/ (accessed: 10.03.2019)

102. Pande J. Introduction to Cyber Security. - Uttarakhand Open University, 2017. - 152 p.

103. Rauscher K. F., Yaschenko V. Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations // [Electronic resource] URL: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng= en&id=130080 (accessed: 13.03.2019)

104. Robertson J., Diab A. Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence // FALL. 2016. [Electronic resource] URL: https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Darknet_Mining_and_Game_Theory_Robertson_et_al.pdf?ver=2018-08-01-090210-620(accessed: 22.03.2019)

105. Rueter N. The Cybersecurity Dilemma. Department of political science Duke University // [Electronic resource] URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.826.7847&rep=rep1&type=pdf (accessed: 10.03.2019)

106. Salim H. Cyber safety: A systems thinking and systems theory approach to managing cyber security risks. - Massachusetts Institute of Technology, 2014. - 157 p.

107. Solms R. From information security to cyber security // Computer & Security. - 2013. - Vol 2. - P. 97-103.

108. Tallinn Manual on the International Law Applicable to Cyber Warfare / ed. Schmitt M. - Cambridge University Press, 2013.

109. The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations 2 / ed. J. B. Godwin III, A. Kulpin, K. F. Rauscher, V. Yaschenko // [Electronic resource] URL: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=178418&lng=en (accessed: 14.03.2019)

110. Vishik C. Key Concepts in Cyber Security // [Electronic resource] URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch11.pdf (accessed: 23.02.2019)

111. Von Solms R. From information security to cyber security // Computers & security. – 2013. – Vol. 38. – P. 97–102.

112. Weimann G. Cyberterrorism: How Real is the Threat? / United States Institute of Peace Special Report 119 (2004). // [Electronic resource] URL: http://www.usip.org/publications/cyberterrorism-how-real-threat (accessed: 05.03.2019)