Третьяков Артемий

Глобальные тенденции в сфере международной информационной безопасности в условиях фрагментации Интернета.

Фрагментация Интернета - это процесс постепенного разделения сети на ряд сегментов киберпространства, независимых друг от друга. Он был описан ещё в в 2001 г. К. У. Крюсом, экспертом американского аналитического центра Cato Institute в виде концепции «сплинтернета»[1]. Согласно исследованию института Брукингса фрагментация происходит в течении последних 15 лет и является отражением кризиса глобализации в международных отношениях[2]. Процесс имеет различные измерения - технологическое, политическое и экономическое, но наибольшие риски он несёт в сфере информационной безопасности.

Модель глобального открытого Интернета с точки зрения информационной безопасности подвергается постепенной дискредитации на основе пяти факторов. **Первый фактор - осознание иллюзии нейтральности сетевой среды.** Этот фактор стал особенно активно влиять на политику в сфере информационной безопасности в 2013 г., когда бывший подрядчик ЦРУ и АНБ Э. Сноуден передал СМИ информацию об использовании США информационных коммуникаций для слежки за гражданами всего мира. В работе Б. Шнайера «Данные и Голиаф» (2015) выдвинут тезис, согласно которому с этого момента ведущие страны мира ускорили разработку законодательных норм для обеспечения технологического суверенитета[3]. В результате были реализованы такие инициативы как Общий регламент по защите данных (GDPR) и запуск проекта GAIA-X в Европе, Закон о хранении медицинских данных и Новая стратегия цифрового правительства в Австралии и др.[4]

Вторым фактором стало распространение вредоносного программного обеспечения и масштабные кибератаки, приписываемые государственным структурам, такие как операция «Орчард» 2006 г., «Олимпийские игры» 2006 г., Stuxnet

---

[1] Crews C. W. One Internet Is Not Enough // Cato Institute. 2001. URL: https://www.cato.org/techknowledge/one-internet-not-enough

[2] Merill N. Komaitis K. The consequences of a fragmenting, less global internet // Brookings. 2020. URL: https://www.brookings.edu/techstream/the-consequences-of-a-fragmenting-less-global-internet/

[3] Schneier B. Data anf Goliaph // W. W. Norton & Company. 2015. URL: https://www.schneier.com/books/data-and-goliath/

[4] Chander A. Uyen P. Le. Data Nationalism // Emory Law Journal, Vol. 64, No. 3, 2015

2010 г., Not Petya 2016 г., атаки на Solar Winds и Colonial Pipeline. Следствием этого стало создание в ведущих странах мира оборонительных и наступательных киберструктур, а также открытое признание рядом стран потенциального и фактического проведения кибератак против оппонентов. Так в 2013 г. глава министр обороны Великобритании Ф. Хамонд официально признал что его страна использует свои наступательные кибервозможности[5], а в 2020 г. президент США Д. Трамп публично подтвердил, что Киберкомандование США в 2018 г. провело скрытую кибератаку на российское Агентство интернет-исследований[6]. Подобные действия постепенно разрушали восприятие Интернета как нейтральной и аполитичной среды, где существуют более мягкие законы, чем на международной арене.

Нарастание напряженности в 2022 г. определило ещё ряд факторов, влияющих на международную информационную безопасность и являющихся следствием процессов фрагментации Интернета. **Третьим фактором стало частичное сворачивание сотрудничества между компаниями в сфере кибербезопасности.** Так компания CISCO, чьи продукты были важны для обеспечения информационной безопасности, прекратила работу в России и Белоруссии. Также важным следствием фрагментации стала политизация ряда международных сервисов, таких как GitHub и дискредитация продуктов на основе открытого программного кода. Ряд инструментов типа polyfill, позволяющие исправлять ошибки в программном интерфейсе и добавлять новые функции Интернет-браузерам, стали транслировать политические сообщения при установке их пользователями из РФ, но не были удалены с сервисов npm и Github. Процесс фрагментации интернета и политизации западных сетевых сервисов в сфере приводит к обособлению ведущих вендоров, снижению интенсивности сотрудничества и ухудшению общего уровня международной информационной безопасности.

Четвёртым фактором стал кризис международного сотрудничества в сфере информационной безопасности. Хотя в крайне сложной обстановке переговоры в рамках Рабочей группы открытого состава (РГОС) в ООН оказались относительно устойчивы, а участникам в июле удалось согласовать промежуточный доклад, ряд российских компаний не был допущен на заседание по инициативе США и Украины. Процесс фрагментации

---

[5] UK becomes first state to admit to offensive cyber attack capability // Financial Times. 2013. URL: https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de

[6] Trump confirms 2018 US cyberattack on Russian troll farm // The Hill. 2020. URL: https://thehill.com/policy/cybersecurity/506865-trump-confirms-2018-us-cyberattack-on-russian-troll-farm/

отчасти также затронул саму инфраструктуру Интернета, когда со стороны представителей Украины поступили требования максимально изолировать российский сегмент Интернета. Хотя большинство подобных требований было отвергнуто международными техническими организациями, произошли некоторые исключения. Например, были отменены мероприятия региональной «Группы сетевых операторов Евразии» (ENOG) и RIPE NCC перераспределила средства, выделенные на финансирование этого мероприятия, в связи с чем была потеряна важная переговорная площадка. Ассоциация европейских операторов TLD CENTR приостановила членство в Координационном центре российского отделения RU/РФ, что также стало важным прецедентом. Процесс фрагментации Интернета был ускорен из-за санкций магистральных провайдеров. Крупный поставщик Интернет-услуг Cogent Communications покинул российский рынок в марте 2022 г. Э. Салливан, исполнительный директор Internet Society заявил, что Сеть Cogent не единственная компания, которая уходит из России, однако если магистральные провайдеры продолжат делать это, Интернет станет более хрупким и менее взаимосвязанным[7].

Пятый фактор в сфере международной информационной безопасности в условиях фрагментации Интернета - это отсутствие реакции на атаки на критическую инфраструктуру. Эта тенденция проявляется в рамках следующих параллельных процессов - затруднение двустороннего диалога США с РФ по вопросам кибербезопасности и ответственного поведения государств в киберпространстве, мобилизация сетевой инфраструктуры западных стран под предлогом защиты от мнимых кибератак со стороны российских хакеров, игнорирование и косвенная поддержка украинских хакерских группировок, совершающих кибератаки на российскую критическую инфраструктуру.

С. Соесанто, эксперт Швейцарской Высшей технической школы Цюриха утверждает, что такие группировки как «IT-армия Украины» превратились в гибридную киберструктуру с неопределённым правовым статусом. Особенно опасным становится участие представителей европейских IT-компаний в деятельности этой структуры (Например главный офис компании Hacken.io, которая помогает хакерам, находится в

---

[7] Russian Internet Takes a Hit as Cogent Cuts Off Its Backbone Network // CNET. 2022. URL: https://www.cnet.com/news/russian-internet-takes-a-hit-as-cogent-cuts-off-its-backbone-network/

Эстонии)[8]. Следует отметить, что один из создателей «IT-армии Украины», министр цифровой трансформации М. Фёдоров получил две награды на Европейском форуме кибербезопасности CYBERSEC 2022 в Катовице (Польша) за «защиту цифровых границ демократического мира»[9]. Отказ от осуждения этих хакерских группировок и от санкций в отношении западных компаний, помогающих им означает фактическую легализацию кибератак на критическую инфраструктуру и максимальное осложнение диалога о принципах ответственного поведения государств в киберпространстве[10]. А политизация сетевых корпораций и сервисов многократно ускоряет процесс фрагментации Интернета, вынуждая создавать альтернативные сервисы и максимально изолировать данные пользователей от иностранных акторов.

Процесс фрагментации Интернета многократно повышает риски в сфере международной информационной безопасности создавая опасные прецеденты нарушения нейтральности международных технических организаций (так один из руководителей ICANN Й. Марби выступил против российского кандидата на пост генерального секретаря Международного союза электросвязи и заявил: «Мы не политическая организация, но однажды мы вмешиваемся… когда мы видим предложения, которые отключат людей от Интернета или фактически лишат вас возможности находиться здесь и участвовать в управлении, именно тогда мы выступаем и реагируем. Это единственный раз»[11]). Ещё более опасным прецедентом становится фактически нейтральное отношение к кибератакам хакерских группировок на критическую инфраструктуру. К сожалению, данная проблема не может быть решена посредством отката назад, к иллюзиям о нейтральном и глобальном Интернете с минимальным вмешательством государств. **Как ни парадоксально, к стабилизации в сфере информационной безопасности скорее всего приведёт дальнейшая фрагментация Интернета и создание киберпространственных блоков, которые уравновешивают потенциал друг друга.**

---

[8] Adam Janofsky, “This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites // The Record. 2022, URL: https://therecord.media/this-ukrainiancyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/.

[9] Ukraine received two awards in the field of cybersecurity at the CYBERSEC European Cybersecurity Forum // Odessa-journal. 2022. URL: https://odessa-journal.com/ukraine-received-two-awards-in-the-field-of-cybersecurity-at-thecybersec-european-cybersecurity-forum/.

[10] Soesanto S. The IT Army of Ukraine // ETH Zurich. 2022. URL: https://css.ethz.ch/en/center/CSS-news/2022/06/the-it-army-of-ukraine.html

[11] Murphy K. ICANN to “stand up” to Russia at the ITU // Domain Incite. 2022. URL: https://domainincite.com/28260-icann-to-stand-up-to-russia-at-the-itu?utm_source=rss&utm_medium=rss&utm_campaign=icann-to-stand-up-to-russia-at-the-itu

Первый шаг к такому блоку уже сформулирован американскими экспертами[12], которые предлагают создать Международный центр киберпреступности, куда войдут США и их союзники, разделяющие общие ценности. Центр будет координировать работу киберструктур этих стран, распределять инвестиции на развитие национальных систем информационной безопасности и собирать информацию о сетевых угрозах. Ответным шагом, который многократно ускорит процесс фрагментации Интернета, но позволит уравновесить эту инициативу, может стать создание аналогичного центра кибербезопасности на площадке ШОС.

Список источников

1. Murphy K. ICANN to “stand up” to Russia at the ITU // Domain Incite. 2022. URL: https://domainincite.com/28260-icann-to-stand-up-to-russia-at-the-itu?utm_source=rss&utm_medium=rss&utm_campaign=icann-to-stand-up-to-russia-at-the-itu
2. Chander A. Uyen P. Le. Data Nationalism // Emory Law Journal, Vol. 64, No. 3, 2015
3. Crews C. W. One Internet Is Not Enough // Cato Institute. 2001. URL: https://www.cato.org/techknowledge/one-internet-not-enough
4. Janofsky A. “This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites // The Record. 2022, URL: https://therecord.media/this-ukrainiancyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/.
5. Merill N. Komaitis K. The consequences of a fragmenting, less global internet // Brookings. 2020. URL: https://www.brookings.edu/techstream/the-consequences-of-a-fragmenting-less-global-internet/
6. Schneier B. Data anf Goliaph // W. W. Norton & Company. 2015. URL: https://www.schneier.com/books/data-and-goliath/
7. Soesanto S. The IT Army of Ukraine // ETH Zurich. 2022. URL: https://css.ethz.ch/en/center/CSS-news/2022/06/the-it-army-of-ukraine.html
8. Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet // Council on Foreign Relations. 2022. URL: https://www.cfr.org/report/confronting-reality-in-cyberspace
9. Russian Internet Takes a Hit as Cogent Cuts Off Its Backbone Network // CNET. 2022. URL: https://www.cnet.com/news/russian-internet-takes-a-hit-as-cogent-cuts-off-its-backbone-network/
10. UK becomes first state to admit to offensive cyber attack capability // Financial Times. 2013. URL: https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de
11. Trump confirms 2018 US cyberattack on Russian troll farm // The Hill. 2020. URL: https://thehill.com/policy/cybersecurity/506865-trump-confirms-2018-us-cyberattack-on-russian-troll-farm/
12. UK becomes first state to admit to offensive cyber attack capability // Financial Times. 2013. URL: https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de
13. Trump confirms 2018 US cyberattack on Russian troll farm // The Hill. 2020. URL: https://thehill.com/policy/cybersecurity/506865-trump-confirms-2018-us-cyberattack-on-russian-troll-farm/
14. Ukraine received two awards in the field of cybersecurity at the CYBERSEC European Cybersecurity Forum // Odessa-journal. 2022. URL: https://odessa-journal.com/ukraine-received-two-awards-in-the-field-of-cybersecurity-at-thecybersec-european-cybersecurity-forum/.

[12] Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet // Council on Foreign Relations. 2022. URL: https://www.cfr.org/report/confronting-reality-in-cyberspace