Сона Де Апро

Кибербезопасность и киберпреступность: единые правила или цифровой суверенитет?

«Свобода одного заканчивается там,
где начинается свобода другого»
(М. Бакунин)

Сегодня на мировой арене одной из самых обсуждаемых тем является сфера кибербезопасности. Высокий уровень интереса к данной сфере объясняется естественным проникновением и уже вполне органичной и необходимой интеграцией киберпространства во все процессы государственного, экономического, социального развития, эффективность которых во многом зависит от него. Вместе с тем, с развитием технологий и прочным внедрением киберпространства в жизнедеятельность государств, бизнеса и гражданского общества наблюдается существенный рост киберпреступности, ведущий к нарушению баланса в киберпространтсве, последствия которого перетекают и в физический мир.

Согласно докладу Всемирного экономического форума[i], киберпреступления входят в ТОП-5 глобальных рисков наряду с терроризмом и глобальным потеплением. По данным МИД России[ii], ущерб от киберпреступлений в 2021 году может достичь 6 трлн. долл. США, а к 2022 году, согласно ВЭФ, сумма всемирного экономического ущерба от кибератак может достигнуть 8 трлн. долл. США. Жертвами кибератак, которые, в свою очередь, с каждым днем приобретают новые, более усовершенствованные формы, становятся государства, компании и организации любых масштабов, а также обычные пользователи.

Попытки национального и всемирного регулирования киберпространства, а также разработка единых стандартов предпринимается уже не первый год и не первое десятилетие. Ключевым вызовом для полноценного и наиболее эффективного правового регулирования киберпространства является его трансграничность. Сложность определения юрисдикции в информационно-коммуникационной сети «Интернет» обуславливается единством и глобальностью киберпространства. Сегодня процесс разработки норм как на национальном, так и на глобальном, в том числе двустороннем, многостороннем уровнях, а также с участием стейкхолдеров из разных секторов продолжается, однако достичь консенсуса удается далеко не всегда.

Так, еще в 2001 году 23 ноября в Будапеште была принята Конвенция [iii] о компьютерных преступлениях, которая стала единственным на сегодняшний день многосторонним договором по борьбе с преступной деятельностью, осуществляемой с помощью информационных технологий. В данной Конвенции предложены меры относительно следующих преступлений: противозаконное использование устройств, преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; воздействие на данные и на функционирование систем; нарушение авторских и смежных прав; правонарушения, связанные с детской порнографией и др. Указанные в Конвенции виды преступлений актуальны и сегодня, однако за последние 20 лет количество киберпреступлений и их видов только увеличилось (например, появились фишинг, вишинг (телефонное мошенничество), вирусы-шифровальщики и др.). К тому же,

Конвенция содержит в себе неприемлемую некоторыми государствами, в частности для России, статью 32b, в которой заявляется, что: «Сторона может без согласия другой Стороны: <...> b) получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему». Данная статья позволяет государствам-участникам без уведомления получать доступ к информации, хранящейся в другом государстве в случае наличия добровольного согласия лица, у которой есть законные полномочия для раскрытия такой информации посредством использования компьютерных технологий. Такая возможность способна нанести прямой удар по цифровому суверенитету — основе независимости государства в киберпространстве.[iv]

В стремлении государств выработать совместными усилиями единые международно-правовые нормы для участников киберпространства просматривается также острая потребность в сохранении и укреплении собственного цифрового суверенитета. Россия и Китай развивают это направление, разрабатывая национальное законодательство. Так, например, в российское законодательство внесен ряд изменений в ФЗ «О связи» и «Об информации», в частности приняты такие законы, как о «суверенном Рунете» [v], «о приземлении» [vi] и др. Изменения касаются не только вопроса укрепления цифрового суверенитета и создания суверенного национального сегмента интернета, но и находят колоссальное отражение в экономическом аспекте. Так, например, сегодня государства стремятся на основе национального законодательства обязать IT-гигантов уплачивать налоги в странах, в которых эти компании оказывают услуги и получают сверхприбыль.

Важно отметить, что на уровне IT-корпораций существует успешный опыт в заключении многосторонних соглашений. В 2018 году было подписано Технологическое соглашение по кибербезопасности (Cybersecurity Tech Accord) [vii] – договор между 34 международными компаниями в сфере технологий и обеспечения безопасности (в том числе Cisco, ABB, Microsoft Corp., HP, Facebook, Oracle, Nokia, Trend Micro, Arm и др.). В рамках соглашения компании обязуются защищать своих клиентов по всему миру от кибератак. Данный документ олицетворяет единство крупнейших в истории технологических корпораций, сумев объединить их ресурсы, мощности и ценный, многолетний опыт ведения деятельности в киберпространстве. На сегодняшний день количество компаний-подписантов данного документа насчитывается более 100.

На уровне государств еще в 2016 году Россия представила проект Конвенции Организации Объединенных Наций «О сотрудничестве в сфере противодействия информационной преступности». Проект был предложен в виде полноценной универсальной международно-правовой базы сотрудничества и единой терминологии, включив в себя достаточно широкий понятийный аппарат и определив такие понятия, как «информация», «информационно-коммуникационные технологии» (ИКТ), «бот-сеть», «объекты критической инфраструктуры» и др. Ст. 57 данной Конвенции предусматривает создание каждым государством-участником ООН круглосуточного центра по реагированию и оперативному содействию в целях оперативного совместного противодействия киберпреступлениям.

Говоря о предложенной Конвенции, следует отметить, что хотя проект был переведен с русского языка на официальные языки ООН, а 28 декабря 2017 г. представлен в виде официального документа Генеральной Ассамблеи ООН по п. 107 повестки дня ее 72-й сессии «Предупреждение преступности и уголовное правосудие», в конечном итоге он не получил общего одобрения. Происходит противостояние не только в отношении данного проекта Конвенции, но и в отношении разработки любых других международно-правовых предложений. Государства аргументируют это наличием Конвенции о компьютерных преступлениях, принятой еще в 2001 году. Очевидно, что в невозможности достичь консенсуса и всестороннего согласия кроется, скорее, вполне осознанное противостояние, которое вот уже 20 лет оттягивает появление новой международно-правовой базы. Ведь наравне с мирными дипломатическими переговорами между государствами по поводу возможности разработки единых правил происходят регулярные кибератаки на критическую инфраструктуру, наносящие ущерб цифровому суверенитету тому или иному государству.

В июле 2021 года США, ЕС и НАТО обвинили Китай в совершении кибератак через Microsoft Exchange. В свою очередь президент США Джо Байден допустил возможность кибератак в ответ на действия российских хакеров. Киберпространство является не только средством для «передвижения» информации, ведения деятельности представителями разных секторов, но и геополитической «великой шахматной доской»[viii]. На кону вопрос технологического лидерства. По этому поводу в своей статье для Financial Times известный политолог Збигнев Бжезинский писал следующее: «Система международных отношений оказалось сейчас в опасности. В течение двух последних веков человечество придерживалось подхода, выработанного на Венском конгрессе в определении состояния войны и мира. Однако сейчас с развитием новейших технологий грань между ними стирается»[ix]. Кроме того, Бжезинский справедливо отмечает, что сегодня США сохраняют «абсолютное лидерство» в технологическом плане. Сегодня на международно-правовом поле отсутствует единый понятийный аппарат в сфере регулирования киберпространства, что усложняет процесс выработки единых международно-правовых норм.

В этом отношении можно вернуться к Технологическому соглашению по кибербезопасности. Данный пример демонстрирует готовность IT-корпораций как представителей отдельной группы стейкхолдеров самостоятельно выработать и принять для себя «внутренние» правила, которым они готовы следовать. «Этический кодекс» сформирован даже среди хакерских группировок (например, «Конвенция самодисциплинирования хакеров»[x], выпущенная в 2011 году китайскими хактивистами). Наличие единого этического кодекса как универсального международного «кодекса поведения» в киберпространстве для правового противодействия использованию информационно-коммуникационных технологий в незаконных целях, а также выработка единой терминологии, которая будет использоваться государствами в ходе правовой имплементации необходимы. В ином случае уровень уязвимости киберпространства, в котором происходящие инциденты перетекают в том числе в реальную жизнь, нанося реальный (материальный, морально-психологический) ущерб, будет только увеличиваться, что приведет к ослаблению устойчивости и замедлению научно-технического, и социально-экономического развития всех без исключения государств.

Таким образом, продолжение совместной работы государств в выработке единых правил поведения, а также единой терминологии сегодня является острой потребностью, что позволит гармонизировать международное, а также национальное законодательства, более эффективней содействовать взаимной правовой помощи, работать над совершенствованием отечественных разработок в области кибербезопасности и наращивать технологический потенциал стран и сплоченно противостоять общему злу в виде киберпреступлений, заранее предотвращая возможность их осуществления. Глобальные правила помогут очертить «границы дозволенного», установить в том числе юридическую ответственность в условиях трансграничности, что объединит усилия государств в отношении борьбы с киберпреступностью, усилит мировую кибербезопасность, а также приведет к укреплению цифрового суверенитета, когда каждое государство будет относиться к безопасности, устойчивости и целостности цифрового суверенитета другого государства как к собственному, выражая уважение к его правам и свободам и готовность прийти на помощь в нужный час.

[i] Доклад ВЭФ, 2021 / Официальный сайт Всемирного экономического форума. https://www.weforum.org
[ii] Дмитрий Малов. МИД оценил ущерб, который киберпреступность может нанести в 2021 году, Газета.ру, 2021. https://www.gazeta.ru/social/news/2021/08/02/n_16329536.shtml
[iii] Конвенция о компьютерных преступлениях (Будапешт, 23 ноября 2001 г.). https://www.refworld.org.ru/pdfid/53020e6b4.pdf
[iv] Данельян А.А. Международно-правовое регулирование киберпространства, 2020. https://education.law-books.ru/данельян-а-а-международно-правовое-ре/
[v] Федеральный закон от 01.05.2019 №90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» http://www.consultant.ru/document/cons_doc_LAW_323815/
[vi] Федеральный закон от 01.07.2021 № 236-ФЗ "О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации" http://publication.pravo.gov.ru/Document/View/0001202107010014
[vii] Технологическое соглашение по кибербезопасности (Cybersecurity Tech Accord), 2018. https://cybertechaccord.org/accord/
[viii] Бжезинский З. «Великая шахматная доска», 1997.
[ix] Збигнев Бжезинский. Кибератаки и угроза хаоса, Financial Times, 2013. https://www.ft.com/topics/people/Zbigniew_Brzezinski
[x] В Китае появится кодекс чести хакера, SecurityLab, 2011. https://www.securitylab.ru/news/407357.php

Список источников

1. Федеральный закон от 01.05.2019 №90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_323815/
2. Федеральный закон от 01.07.2021 № 236-ФЗ "О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации" [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202107010014

3. Конвенция о преступности в сфере компьютерной информации ETS No 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. URL: https:// base.garant.ru/4089723/
4. Резолюция Генеральной Ассамблеи ООН 74/247 от 29 декабря 2019 года «Противодействие использованию информационно-коммуникационных технологий в преступных целях»
5. Технологическое соглашение по кибербезопасности (Cybersecurity Tech Accord [Электронный ресурс]. URL: https://cybertechaccord.org/accord/
6. Киберпространство как стратегический инструмент социальной инженерии. URL: https:// whatisgood.ru/theory/analytics/kiberprostranstvo- kak-strategicheskiy-instrument/
7. Бжезинский З. «Великая шахматная доска»
8. Курбалийя Й., Гелбстайн Э. Управление Интернетом: проблемы, субъекты, преграды // [Электронный ресурс]. URL: http://www.ifap.ru/library/book178.pdf/
9. Madiega T. Digital sovereignty for Europe. EPRS Ideas Paper Towards a more resilient EU. July 2020 // http://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf/
10. Terminal neutrality as a tool for our digital sovereignty? // La Tribune. April 2020 // [Электронный ресурс]. URL: http://www.web24.news/u/2020/04/terminal-neutrality-as-a-tool-for-our-digital-sovereignty.html/
11. Yeli H. A Three-Perspective Theory of Cyber Sovereignty // [Электронный ресурс]. URL:http://www.cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/10-3-Perspective%20Theory.pdf/
12. В Китае появится кодекс чести хакера, 2011. [Электронный ресурс]. URL: https://www.securitylab.ru/news/407357.php
13. Дмитрий Малов. МИД оценил ущерб, который киберпреступность может нанести в 2021 году, Газета.ру, 2021. [Электронный ресурс]. URL: https://www.gazeta.ru/social/news/2021/08/02/n_16329536.shtml
14. Доклад ВЭФ, 2021 / Официальный сайт Всемирного экономического форума. [Электронный ресурс]. URL: https://www.weforum.org